世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 **H04L 9/08, 9/14, 9/32, H04H 1/00**	**A1**	(11) 国際公開番号 **WO99/50992** (43) 国際公開日 1999年10月7日(07.10.99)

(21) 国際出願番号 PCT/JP99/01606

(22) 国際出願日 1999年3月30日(30.03.99)

(30) 優先権データ

特願平10/89098	1998年4月1日(01.04.98)	JP
特願平10/161082	1998年6月9日(09.06.98)	JP
特願平10/162667	1998年6月10日(10.06.98)	JP

(71) 出願人（米国を除くすべての指定国について）
松下電器産業株式会社
(MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP]
〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
西村拓也(NISHIMURA, Takuya)[JP/JP]
〒545-0053 大阪府大阪市阿倍野区松崎町3-9-18-F Osaka, (JP)
飯塚裕之(IITSUKA, Hiroyuki)[JP/JP]
〒576-0033 大阪府交野市私市6-25-6 Osaka, (JP)
山田正純(YAMADA, Masazumi)[JP/JP]
〒570-0011 大阪府守口市金田町6-24-10 Osaka, (JP)
後藤昌一(GOTOH, Shoichi)[JP/JP]
〒576-0021 大阪府交野市妙見坂5-4-204 Osaka, (JP)
武知秀明(TAKECHI, Hideaki)[JP/JP]
〒533-0004 大阪府大阪市東淀川区小松4丁目11-10
レモンフラッツ201 Osaka, (JP)
(74) 代理人
弁理士 松田正道(MATSUDA, Masamichi)
〒532-0003 大阪府大阪市淀川区宮原5丁目1番3号
新大阪生島ビル Osaka, (JP)

(81) 指定国 CN, KR, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

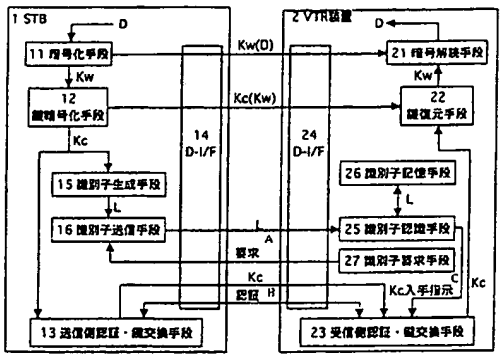
添付公開書類
国際調査報告書
補正書

(54)Title: **DATA TRANSMITTING/RECEIVING METHOD, DATA TRANSMITTER, DATA RECEIVER, DATA TRANSMITTING/RECEIVING SYSTEM, AV CONTENT TRANSMITTING METHOD, AV CONTENT RECEIVING METHOD, AV CONTENT TRANSMITTER, AV CONTENT RECEIVER, AND PROGRAM RECORDING MEDIUM**

(54)発明の名称 データ送受信方法、データ送信装置、データ受信装置、データ送受信システム、AVコンテンツ送信方法、AVコンテンツ受信方法、AVコンテンツ送信装置、AVコンテンツ受信装置およびプログラム記録媒体

(57) Abstract

A data transmitting/receiving method ensuring a high security enhanced by control key update and a high transmission/reception efficiency enhanced by reducing the numbers of authentications and key exchanges. An STB (1) transmits encrypted digital data (Kw(D)) encrypted from digital data (D) using a work key (Kw) and an encrypted work key (Kc(Kw)) encrypted from the work key (Kw) using a control key (Kc), regularly or irregularly updates the control key (Kc), and imparts an identifier (L) for identifying the control key (Kc) to every control key (Kc). A VTR apparatus (2) decrypts the received control key (Kc(Kw)) with the control key (Kc) obtained by performing authentication and key exchange with the STB1, decrypts the received work key (Kw(D)) with the control key (Kc(Kw)), obtains the digital data (D), refers to the transmitted identifier (L) when it resumes the reception after the reception is suspended, judges whether or not the control key (Kc) is updated while the reception is suspended, performs authentication and key exchange again if the control key (Kc) is judged to be updated, and thus obtains the updated control key (Kc).



2 ... VTR APPARATUS
11 ... ENCRYPTING MEANS
12 ... KEY ENCRYPTING MEANS
13 ... TRANSMISSION-SIDE AUTHENTICATING/KEY EXCHANGING MEANS
15 ... IDENTIFIER GENERATING MEANS
16 ... IDENTIFIER TRANSMITTING MEANS
21 ... ENCRYPTING MEANS
22 ... KEY RESTORING MEANS
23 ... RECEPTION-SIDE AUTHENTICATING/KEY EXCHANGING MEANS
25 ... IDENTIFIER RECOGNIZING MEANS
26 ... IDENTIFIER STORAGE MEANS
27 ... IDENTIFIER REQUESTING MEANS

A ... REQUEST
B ... AUTHENTICATION
C ... INSTRUCTION TO OBTAIN Kc

(57)要約

コントロールキー更新によりセキュリティを高め、認証・鍵交換の回数を減らすことにより、送受信効率を高めるデータ送受信方法を提供する。ＳＴＢ１は、ディジタルデータＤにワークキーＫｗを用いて暗号化した暗号化ディジタルデータＫｗ（Ｄ）と、ＫｗにコントロールキーＫｃを用いて暗号化した暗号化ワークキーＫｃ（Ｋｗ）とを送信し、Ｋｃを定期的または不定期的に更新するとともに、Ｋｃ毎にＫｃを特定できる識別子Ｌを付与し、ＶＴＲ装置２は、ＳＴＢ１と認証・鍵交換を行って得たＫｃを用いて、受信したＫｃ（Ｋｗ）を解読し、このＫｗを用いて受信したＫｗ（Ｄ）を解読して、Ｄを得、受信中断後に受信を再開する際に、送信されてきたＬを参照することにより、受信中断中にＫｃが更新されたか否かを判断し、Ｋｃが更新されたと判断した場合には、前記認証・鍵交換を改めて行うことによって、更新後のＫｃを得る。

明　細　書

データ送受信方法、データ送信装置、データ受信装置、データ送受信システム、ＡＶコンテンツ送信方法、ＡＶコンテンツ受信方法、ＡＶコンテンツ送信装置、ＡＶコンテンツ受信装置およびプログラム記録媒体

技術分野

本発明は、データ送受信方法、データ送信装置、データ受信装置、データ送受信システムおよび前記各装置に備えられた手段の機能の全部または一部をコンピュータに実行させるプログラムを格納する媒体に関するものである。

また、本発明は、異なる暗号化手法で暗号化されたＡＶコンテンツの送信と、そのＡＶコンテンツの受信とに関するものである。

背景技術

従来技術として、第１の従来技術と、第２の従来技術とがあるので、それぞれを順番に説明する。

先ず、第１の従来技術を述べる。特定のユーザー、特定の機器等に対してのみ、データを提供する場合、提供対象以外の人間、機器に当該データを利用できなくする方法として、送信側がデータを暗号化して送信し、受信側が暗号化されたデータを解読して使用する方法がある。

上記の方法について、衛星放送のＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ；衛星放送受信機）から当該衛星放送データを録画するＶＴＲ装置へのデータの送受信方法を例にとって、以下に説明する。本方法は、衛星放送の録画契約の対象となっているＶＴＲ装置にのみ、正しい衛星放送データを録画させるた

めに、暗号化を行うものである。

図１４は、衛星放送のＳＴＢをデータ送信装置とし、ＶＴＲ装置をデータ受信装置とした場合の従来のデータ送受信システムを示す構成図である。なお、本構成図は、ＳＴＢとＶＴＲ装置とのデータの送受信に関する構成要素のみを示したものであり、ＳＴＢにおける衛星からの受信手段等、ＶＴＲ装置における記録媒体への記録手段等については、図示を省略している。本システムは、衛星から受信した電波をＡＶデータに変換して、ＶＴＲ装置１０２へ送信するＳＴＢ１０１、ＳＴＢ１０１から送信されてきた前記ＡＶデータを記録媒体に記録するＶＴＲ装置１０２から構成されている。

ＳＴＢ１０１は、ワークキーＫｗを定期的または不定期的に更新生成し、衛星から受信した電波をＡＶデータに変換して得られたディジタルデータＤに、ワークキーＫｗを用いて第１の暗号化を施して暗号化ディジタルデータＫｗ（Ｄ）に変換して、ＶＴＲ装置１０２へ送信する暗号化手段１１１と、コントロールキーＫｃを生成し、ワークキーＫｗにコントロールキーＫｃを用いて第２の暗号化を施して暗号化ワークキーＫｃ（Ｋｗ）に変換して、ＶＴＲ装置１０２へ送信する鍵暗号化手段１１２と、ＶＴＲ装置１０２との認証・鍵交換を行う送信側認証・鍵交換手段１１３と、ＶＴＲ装置１０２のＤ－Ｉ／Ｆ１２４と直接データの伝達を行うＤ－Ｉ／Ｆ（ディジタルインターフェイス）１１４とを備えている。

ＶＴＲ装置１０２は、ＳＴＢ１０１のＤ－Ｉ／Ｆ１１４と直接データの伝達を行うＤ－Ｉ／Ｆ１２４と、ＳＴＢ１０１の送信側認証・鍵交換手段１１３との認証・鍵交換を行う受信側認証・鍵交換手段１２３と、暗号化ワークキーＫｃ（Ｋｗ）を、受信側認証・鍵交換手段１２３を介して得られたコン

トロールキーＫｃを用いて解読して、ワークキーＫｗを復元する鍵復元手段１２２と、暗号化ディジタルデータＫｗ（Ｄ）を、鍵復元手段１２２によって復元されたワークキーＫｗを用いて解読して、ディジタルデータＤを復元する暗号解読手段１２１とを備えている。

ＳＴＢ１０１からＶＴＲ装置１０２へ送信されるデータは、暗号化ディジタルデータＫｗ（Ｄ）、暗号化ワークキーＫｃ（Ｋｗ）およびコントロールキーＫｃであるが、暗号化ディジタルデータＫｗ（Ｄ）および暗号化ワークキーＫｃ（Ｋｗ）は、暗号化されたデータであり、コントロールキーＫｃは、送信側認証・鍵交換手段１１３と受信側認証・鍵交換手段１２３との間で認証を行った後に、送信されるものであるから、不正にデータを利用しようとする第三者に対しては、セキュリティーの高いシステムとなっている。

次に、第２の従来技術を述べる。上述したように、近年、映画等のＡＶコンテンツ（ＡＶデータ）をディジタル信号を用いて送信し、そのＡＶコンテンツを受信するといったことに関する技術が進歩してきている。

そのようなＡＶコンテンツを送信する送信装置は、ＡＶコンテンツを送信する前に、内容を保護するという目的のために、ＡＶコンテンツの暗号化を行う。そして、受信装置は、暗号化されたＡＶコンテンツを受信し解読して、そのＡＶコンテンツの内容をモニタに表示する。

さて、上述したように、送信装置はＡＶコンテンツを暗号化するが、その暗号化に用いる暗号化手法には、複数の種類がある。例えば、受信装置がテレビ等の通常の家電機器であれば、そのような家電機器に対応させて、Ｍ６、Ｂlowfish 等の'baseline cipher'と呼ばれる「基本暗号化手法」が用いられる。それに対 して、例えば、受信装置がパソコン等の演算能力の高い機器

であれば、ＤＥＳ等の暗号の強度がより高く、より複雑な「拡張暗号化手法」が用いられる。

従来技術と同様に、課題も第１の従来技術と、第２の従来技術とにそれぞれ対応して存在するので、それぞれの課題を順番に説明する。

先ず、第１の従来技術に対する課題を述べる。上述したように、コントロールキーＫｃは、認証を行った後送信されるものであるが、同じＫｃをずっと使用していると、第三者によってＫｃが解読されてしまう可能性が高くなるため、Ｋｃを定期的または不定期的に更新することによって、よりセキュリティーの高いシステムとすることが考えられるが、Ｋｃの更新の度に認証・鍵交換を実行する必要があるため、システムに与える負荷を低減し、送受信効率を高めるという観点から、認証・鍵交換の回数をできるだけ減らすことが求められている。

図１５は、従来のデータ送受信システムにおいて、コントロールキーを更新するとした場合の、コントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。図の横方向は、時間の経過を表し、一段目の帯は、ＳＴＢがデータ信号を送信中であることを示す。２段目の矢印は、同じコントロールキーＫｃが使用されている範囲を示し、本図では途中でＫｃ［１］からＫｃ［２］に更新されたことを示している。３～５段目の帯は、各ケースにおけるＶＴＲ装置が受信状態であることを示し、帯が途切れている範囲は、受信が中断状態であることを示す。また、３～５段目の縦向きの両矢印は、認証・鍵交換が実行されたことを示す。

ケース１のＶＴＲ装置は、受信開始後に受信中断がないため、受信開始時に認証・鍵交換を実行し、以後は、コントロールキーＫｃの更新時のみに認

証・鍵交換を実行するだけでよい。ケース２およびケース３のＶＴＲ装置は、受信開始後に受信中断が起こったため、受信再開時に認証・鍵交換を実行しなければならない。特に、ケース３のＶＴＲ装置においては、中断時間が短かったため、受信再開時にＫｃが更新されていないにも関わらず、改めて認証・鍵交換を実行しなければならず、他のケースに比べてトータルの認証・鍵交換の実行回数が増えることとなる。

本発明は、上述した従来のデータ送受信方法およびデータ送受信システムの課題を考慮し、コントロールキー更新によりセキュリティを高め、認証・鍵交換の実行回数を減らすことによって送受信効率を高めるデータ送受信方法、データ送信装置、データ受信装置、データ送受信システムおよび、前記各装置に備えられた各構成手段の全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したプログラム記録媒体を提供することを目的とするものである。

次に、第２の従来技術に対する課題を述べる。その第２の従来技術を説明するさいに用いた送信装置がパソコン等の演算能力の高い機器であって、ＩＥＥＥ１３９４バスを利用して、ＡＶコンテンツを送信し、そのＩＥＥＥ１３９４バスを介して、受信装置がＡＶコンテンツを受信する場合、上述したように、受信装置がパソコン等の演算能力の高い機器であれば、送信装置は「拡張暗号化手法」を使用してＡＶコンテンツを暗号化し送信しても、受信装置はそのＡＶコンテンツを解読することができるので、何等問題は起こらない。

しかしながら、図１６に示すように、例えば、パソコン５８という受信装置とともに、セットトップボックス（衛星放送受信機）５９のような通常の

家電機器も、ＩＥＥＥ１３９４バスを介して送信装置５７に接続されている場合がある。その場合、送信装置５７が「拡張暗号化手法」を使用してＡＶコンテンツを暗号化して送信し、パソコン５８が受信し解読しているときに、その送信の途中から、セットトップボックス５９がそのＡＶコンテンツを受信し解読しようとしても、セットトップボックス５９は、「拡張暗号化手法」を使用することができないので、そのＡＶコンテンツを解読することができない。

発明の開示

本発明は、上述したように、ＡＶコンテンツ送信装置が第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置がそのＡＶコンテンツを解読することができないという課題を考慮して、ＡＶコンテンツ送信装置が第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置がそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信方法を提供することを目的とするものである。

また、本発明は、第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置がそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信装置を提供することを目的とするものである。

また、本発明は、上述したＡＶコンテンツ送信方法を用いたさい、第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、第１の暗

号化手法を使用することができないＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、その別のＡＶコンテンツ受信装置が引き続きそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信方法およびＡＶコンテンツ受信方法を提供することを目的とするものである。

さらに、本発明は、上述したＡＶコンテンツ送信装置が第１の暗号化手法を使用することができないＡＶコンテンツ受信装置にそのＡＶコンテンツを解読させる場合、そのＡＶコンテンツ受信装置とは別に、第１の暗号化手法で暗号化されていたＡＶコンテンツを引き続き解読するＡＶコンテンツ受信装置を提供することを目的とするものである。

上述した課題を解決するために、第１の本発明（請求項１に対応）は、送信側が、ディジタルデータにワークキーを用いて第１の暗号化を施した暗号化ディジタルデータと、前記ワークキーにコントロールキーを用いて第２の暗号化を施した暗号化ワークキーとを送信し、受信側が、前記送信側と認証・鍵交換を行うことによって得た前記コントロールキーを用いて、受信した前記暗号化ワークキーを解読し、解読して得られた前記ワークキーを用いて受信した前記暗号化ディジタルデータを解読して、前記ディジタルデータを得るデータ送受信方法において、前記送信側は、前記コントロールキーを定期的または不定期的に更新するとともに、前記コントロールキー毎に前記コントロールキーを特定できる識別子を付与し、前記受信側は、受信中断後に受信を再開する際に、前記送信側から送信されてきた前記識別子を参照することにより、前記受信中断中に前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記認証・鍵交換を改めて行うことによって、更新後の前記コントロールキーを得る

ことを特徴とするデータ送受信方法である。

第２の本発明（請求項６に対応）は、ワークキーを定期的または不定期的に更新生成し、ディジタルデータに前記ワークキーを用いて第１の暗号化を施して暗号化ディジタルデータに変換して、データ受信装置へ送信する暗号化手段と、

コントロールキーを定期的または不定期的に更新生成し、前記ワークキーに前記コントロールキーを用いて第２の暗号化を施して暗号化ワークキーに変換して、前記データ受信装置へ送信する鍵暗号化手段と、

前記データ受信装置との認証・鍵交換を行う送信側認証・鍵交換手段と、

前記コントロールキーを特定できる識別子を生成する識別子生成手段と、

前記識別子を前記データ受信装置へ送信する識別子送信手段とを

備えたことを特徴とするデータ送信装置である。

第３の本発明（請求項８に対応）は、データ送信装置との認証・鍵交換を行う受信側認証・鍵交換手段と、

ワークキーにコントロールキーを用いて第２の暗号化を施して変換された暗号化ワークキーを、前記受信側認証・鍵交換手段を介して得られた前記コントロールキーを用いて解読して、前記ワークキーを復元する鍵復元手段と、

ディジタルデータに前記ワークキーを用いて第１の暗号化を施して変換された暗号化ディジタルデータを、前記鍵復元手段によって復元された前記ワークキーを用いて解読して、前記ディジタルデータを復元する暗号解読手段と、

少なくとも、受信中断後に受信を再開する際に、前記データ送信装置から

送信されてきた、前記コントロールキーを特定するための識別子を参照することにより、前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記受信側認証・鍵交換手段に前記認証・鍵交換を改めて行って更新後の前記コントロールキーを得ることを指示する識別子認識手段とを

備えたことを特徴とするデータ受信装置である。

第４の本発明（請求項１４に対応）は、本発明のデータ送信装置および本発明のデータ受信装置を備えたことを特徴とするデータ送受信システムである。

第５の本発明（請求項１５に対応）は、本発明のデータ送信装置およびデータ受信装置が備える各構成手段の全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。

第６の本発明（請求項１６に対応）は、ＡＶコンテンツ送信装置が伝送路を利用して第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、

その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、

その認証要求をしたＡＶコンテンツ受信装置が使用することができる第２の暗号化手法で前記ＡＶコンテンツを暗号化して送信する

ことを特徴とするＡＶコンテンツ送信方法である。

第７の本発明（請求項１７に対応）は、第６の本発明のＡＶコンテンツ送信方法において、

前記認証要求があったさい、既にそれまでの前記第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、前記認証要求をしたＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、

その別のＡＶコンテンツ受信装置に、暗号化手法が前記第２の暗号化手法に切り替わることを通知する

ことを特徴とするＡＶコンテンツ送信方法である。

第８の本発明（請求項１８に対応）は、第７の本発明のＡＶコンテンツ送信方法において、前記暗号化手法の切り替えを、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とするＡＶコンテンツ送信方法である。

第９の本発明（請求項１９に対応）は、第８の本発明のＡＶコンテンツ送信方法において、前記切り替えた後の前記第２の暗号化手法がどのような暗号化手法であるのかという情報を、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とするＡＶコンテンツ送信方法である。

第１０の本発明（請求項２０に対応）は、第８の本発明のＡＶコンテンツ送信方法において、前記切り替えた後の前記第２の暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とするＡＶコンテンツ送信方法である。

第１１の本発明（請求項２１に対応）は、第６の本発明のＡＶコンテンツ送信方法において、前記暗号化手法の切り替えのタイミングを、前記認証要求がある前に使用していた前記第１の暗号化手法での暗号化鍵の更新のタイ

ミングとすることを特徴とするＡＶコンテンツ送信方法である。

第１２の本発明（請求項２２に対応）は、第７の本発明のＡＶコンテンツ送信方法において、少なくとも前記別のＡＶコンテンツ受信装置に、前記暗号化手法が前記第２の暗号化手法に切り替わることを通知するとともに、その暗号化手法の切り替えのタイミングの情報を送信することを特徴とするＡＶコンテンツ送信方法である。

第１３の本発明（請求項２３に対応）は、第６の本発明のＡＶコンテンツ送信方法において、

前記ＡＶコンテンツ送信装置が前記認証要求をしたＡＶコンテンツ受信装置を記憶し、

そのＡＶコンテンツ受信装置から、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなった場合、

前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替える

ことを特徴とするＡＶコンテンツ送信方法である。

第１４の本発明（請求項２４に対応）は、第６の本発明のＡＶコンテンツ送信方法において、

前記ＡＶコンテンツ送信装置が、前記認証要求をしたＡＶコンテンツ受信装置と前記そのＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、

前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を

要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第１の暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、

前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替える

ことを特徴とするＡＶコンテンツ送信方法である。

第１５の本発明（請求項２５に対応）は、第６から第１４のいずれかの本発明のＡＶコンテンツ送信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。

第１６の本発明（請求項２６に対応）は、第６から第１４のいずれかの本発明のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツを受信し、

そのＡＶコンテンツが暗号化されたさいに使用された暗号化手法に基づくとともに、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読する

ことを特徴とするＡＶコンテンツ受信方法である。

第１７の本発明（請求項２７に対応）は、第１６の本発明のＡＶコンテンツ送信方法において、

第６から第１４のいずれかの本発明のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、

その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵

の種との一方または両方が含まれていない場合、

前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記暗号化手法の切り替えに関する情報に含まれていないものを送信するように要求する

ことを特徴とするＡＶコンテンツ受信方法である。

第１８の本発明（請求項２８に対応）は、第１６または第１７の本発明のＡＶコンテンツ受信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。

第１９の本発明（請求項２９に対応）は、送信しようとするＡＶコンテンツを暗号化するさいの暗号化手法を選択する暗号化手法選択手段と、

その暗号化手法選択手段によって選択された暗号化手法に対応した、ＡＶコンテンツを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、

ＡＶコンテンツを入力するとともに、前記暗号化鍵生成手段からの前記暗号化鍵を入力し、その暗号化鍵を利用して、前記ＡＶコンテンツを暗号化する暗号化手段と、

ＡＶコンテンツ受信装置との間で認証・鍵交換を行う送信側認証・鍵交換手段とを備え、

ＡＶコンテンツ送信装置が、前記暗号化手法選択手段によって選択された第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、

その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、前記送信側認証・鍵交換手段が、その認証要求をし

たＡＶコンテンツ受信装置との間で認証を行い、

前記暗号化手法選択手段が、暗号化手法を、前記認証要求をしたＡＶコンテンツ受信装置が使用することができる第２の暗号化手法に切り替える

ことを特徴とするＡＶコンテンツ送信装置である。

第２０の本発明（請求項３０に対応）は、第１９の本発明のＡＶコンテンツ送信装置において、

前記認証要求があったさい、既にそれまでの前記第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、前記認証要求をしたＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、

その別のＡＶコンテンツ受信装置に、暗号化手法が前記第２の暗号化手法に切り替わることを通知する暗号化手法通知手段を備えた

ことを特徴とするＡＶコンテンツ送信装置である。

第２１の本発明（請求項３１に対応）は、第１９の本発明のＡＶコンテンツ送信装置において、

前記暗号化鍵生成手段が、定期的または不定期に前記暗号化鍵を更新し、

前記暗号化手法選択手段が暗号化手法を前記第２の暗号化手法に切り替えるタイミングが、前記暗号化鍵生成手段が前記第１の暗号化手法において暗号化鍵を更新するタイミングである

ことを特徴とするＡＶコンテンツ送信装置である。

第２２の本発明（請求項３２に対応）は、第１９の本発明のＡＶコンテンツ送信装置において、

前記送信側認証・鍵交換手段が、前記認証要求をしたＡＶコンテンツ受信装置を記憶するとともに、そのＡＶコンテンツ受信装置から、前記ＡＶコン

テンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなったと判断した場合、

前記暗号化手法選択手段が、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替える

ことを特徴とするＡＶコンテンツ送信装置である。

第２３の本発明（請求項３３に対応）は、第１９の本発明のＡＶコンテンツ送信装置において、

前記送信側認証・鍵交換手段が、前記認証要求をしたＡＶコンテンツ受信装置と前記そのＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、

前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第１の暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、

前記暗号化手法選択手段が、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替える

ことを特徴とするＡＶコンテンツ送信装置である。

第２４の本発明（請求項３４に対応）は、第１９から第２３のいずれかの本発明のＡＶコンテンツ送信装置との間で認証・鍵交換を行う受信側認証・鍵交換手段と、

前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツのその暗号化に利用された暗号化手法の情報を入力し、記憶する暗号化手法記憶手段

と、

前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツを入力するとともに、前記ＡＶコンテンツ送信装置からの暗号化鍵またはその暗号化鍵の種を入力し、その後、前記暗号化手法記憶手段に記憶されている暗号化手法に基づき、かつ、前記暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読する暗号解読手段とを備えた

ことを特徴とするＡＶコンテンツ受信装置である。

第２５の本発明（請求項３５に対応）は、第２４の本発明のＡＶコンテンツ受信装置において、

第１９から第２３のいずれかの本発明のＡＶコンテンツ送信装置から送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、

その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、

前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記情報に含まれていないものを送信するように要求する要求手段を備えた

ことを特徴とするＡＶコンテンツ受信装置である。

図面の簡単な説明

図１は、本発明の第１の実施の形態におけるデータ送受信システムの構成

を示す構成図である。

図２は、本発明の第１の実施の形態におけるデータ送受信システムにおいて、ＳＴＢ１がデータを暗号化して送信し、ＶＴＲ装置２が暗号化されたデータを解読して使用する方法の手順を示すフロー図である。

図３は、本発明の第１の実施の形態におけるデータ送受信システムにおいて、受信中断が生じ、受信を再開する場合の手順を示すフロー図である。

図４は、本発明の第１の実施の形態におけるデータ送受信システムのコントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。

図５は、本発明の第２の実施の形態におけるデータ送受信システムの構成を示す構成図である。

図６は、本発明の第２の実施の形態におけるデータ送受信システムにおいて、ＳＴＢ１がデータを暗号化して送信し、ＶＴＲ装置２が暗号化されたデータを解読して使用する方法の手順を示すフロー図である。

図７は、本発明の第２の実施の形態におけるデータ送受信システムにおいて、受信中断が生じ、受信を再開する場合の手順を示すフロー図である。

図８は、本発明の第２の実施の形態におけるデータ送受信システムのコントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。

図９は、本発明の第３の実施の形態のＡＶコンテンツ通信システムのブロック図である。

図１０は、本発明の第３の実施の形態のＡＶコンテンツ通信システムのＡＶコンテンツ送信装置３１が送信するＡＶコンテンツおよびコマンドを含むデータの構成図である。

図１１は、本発明の第３の実施の形態のＡＶコンテンツ通信システムのＡ

Ｖコンテンツ送信装置３１の動作の一部を示すフローチャートである。

図１２は、本発明の第３の実施の形態のＡＶコンテンツ通信システムの第１のＡＶコンテンツ受信装置３２の動作の一部を示すフローチャートである。

図１３は、図１１とは異なる、本発明の第３の実施の形態のＡＶコンテンツ通信システムのＡＶコンテンツ送信装置３１の動作の一部を示すフローチャートである。

図１４は、従来のデータ送受信システムを示す構成図である。

図１５は、従来のデータ送受信システムにおいて、コントロールキーを更新するとした場合の、コントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。

図１６は、第２の従来技術の課題を説明するための図である。

（符号の説明）

１、１０１　ＳＴＢ

２、１０２　ＶＴＲ装置

１１、１１１　暗号化手段

１２、１１２　鍵暗号化手段

１３、１１３　送信側認証・鍵交換手段

１４、２４、１１４、１２４　Ｄ－Ｉ／Ｆ

１５　識別子生成手段

１６　識別子送信手段

２１、１２１　暗号解読手段

２２、１２２　鍵復元手段

２３、１２３　受信側認証・鍵交換手段

２５　識別子認識手段

２６　識別子記憶手段

２７　識別子要求手段

３１　ＡＶコンテンツ送信装置

３２　第１のＡＶコンテンツ受信装置

３３　第２のＡＶコンテンツ受信装置

３４　アンテナ

３５、３６　モニタ

３７　受信手段

３８　暗号化手段

３９　Ｋｃｏ生成手段

４０　暗号化手法選択手段

４１、４６、５３　ＡＫＥ手段

４２　暗号化手法変更通知手段

４３　Ｋｃｏ要求コマンド応答手段

４４、４５、５２　データ転送手段

４７　暗号化手法通知検出手段

４８、５４　Ｋｃｏ要求コマンド発行手段

４９、５５　Ｋｃｏ記憶手段

５０　暗号化手法記憶手段

５１、５６　暗号解読手段

５７　送信装置

５８　パソコン

５９　セットトップボックス（衛星放送受信機）

発明を実施するための最良の形態

以下に、本発明の実施の形態を図面を参照して説明する。

（第１の実施の形態）

以下に、本発明の第１の実施の形態を図面を参照して説明する。

図１は、本発明の第１の実施の形態におけるデータ送受信システムの構成を示す構成図である。なお、本構成図は、ＳＴＢとＶＴＲ装置とのデータの送受信に関する構成要素のみを示したものであり、ＳＴＢにおける衛星からの受信手段等、ＶＴＲ装置における記録媒体への記録手段等については、図示を省略している。本実施の形態におけるデータ送受信システムは、衛星放送のＳＴＢから当該衛星放送データを録画するＶＴＲ装置へデータの送受信を行うシステムであり、本発明のデータ送信装置に対応するＳＴＢ１と、本発明のデータ受信装置に対応するＶＴＲ装置２とから構成されている。

ＳＴＢ１は、ワークキーＫｗを定期的または不定期的に更新生成し、衛星から受信した電波をＡＶデータに変換して得られたディジタルデータＤに、ワークキーＫｗを用いて第１の暗号化を施して暗号化ディジタルデータＫｗ（Ｄ）に変換して、ＶＴＲ装置２へ送信する暗号化手段１１と、コントロールキーＫｃを定期的または不定期的に更新生成し、ワークキーＫｗにコントロールキーＫｃを用いて第２の暗号化を施して暗号化ワークキーＫｃ（Ｋｗ）に変換して、ＶＴＲ装置２へ送信する鍵暗号化手段１２と、ＶＴＲ装置２との認証・鍵交換を行う送信側認証・鍵交換手段１３と、ＶＴＲ装置２のＤ

－Ｉ／Ｆ２４と直接データの伝達を行うＤ－Ｉ／Ｆ（ディジタルインターフェイス）１４と、コントロールキーＫｃを特定できる識別子Ｌを生成する識別子生成手段１５と、識別子ＬをＶＴＲ装置２へ送信する識別子送信手段１６とを備えている。

ＶＴＲ装置２は、ＳＴＢ１のＤ－Ｉ／Ｆ１４と直接データの伝達を行うＤ－Ｉ／Ｆ２４と、ＳＴＢ１の送信側認証・鍵交換手段１３との認証・鍵交換を行う受信側認証・鍵交換手段２３と、暗号化ワークキーＫｃ（Ｋｗ）を、受信側認証・鍵交換手段２３を介して得られたコントロールキーＫｃを用いて解読して、ワークキーＫｗを復元する鍵復元手段２２と、暗号化ディジタルデータＫｗ（Ｄ）を、鍵復元手段２２によって復元されたワークキーＫｗを用いて解読して、ディジタルデータＤを復元する暗号解読手段２１と、少なくとも、受信中断後に受信を再開する際に、ＳＴＢ１から送信されてきた、コントロールキーＫｃを特定するための識別子Ｌを参照することにより、コントロールキーＫｃが更新されたか否かを判断し、コントロールキーＫｃが更新されたと判断した場合には、受信側認証・鍵交換手段２３に前記認証・鍵交換を改めて行って更新後のコントロールキーＫｃを得ることを指示する識別子認識手段２５と、送信されてきた識別子Ｌを記憶する識別子記憶手段２６と、前記受信中断後に受信を再開する際に、識別子Ｌを送信することをＳＴＢ１の識別子送信手段１６に対して要求する識別子要求手段２７とを備えている。

なお、Ｄ－Ｉ／Ｆ１４および２４の具体例としては、ＩＥＥＥ１３９４のＤ－Ｉ／Ｆが挙げられる。これは、リアルタイム性の保証が必要となる映像や音声の様なデータの転送に適したアイソクロナス転送と、その必要のない

認証用データやコマンド等の転送に適したアシンクロナス転送の２つの転送を行うものである。

次に、本システムにおいて、ＳＴＢ１がデータを暗号化して送信し、V.TR装置２が暗号化されたデータを解読して使用する方法の手順について、図２、図３を用いて説明する。

まず、通常の送受信時の手順を図２を用いて説明する。図２は、本発明の第１の実施の形態におけるデータ送受信システムにおいて、ＳＴＢ１がデータを暗号化して送信し、ＶＴＲ装置２が暗号化されたデータを解読して使用する方法の手順を示すフロー図である。なお、図２において、左側に、ＳＴＢ１で行われる処理が、右側に、ＶＴＲ装置２で行われる処理が示されている。また、ＳＴＢ１とＶＴＲ装置２との間のデータの送受信は、全てＤ－Ｉ／Ｆ１４および２４を介して行われるが、以下の説明においては、この説明を省略する。

鍵暗号化手段１２は、送信開始と同時にコントロールキーＫｃを生成し（ステップＳ１）、これを送信側認証・鍵交換手段１３および識別子生成手段１５に送る。識別子生成手段１５は、このＫｃを特定するための識別子Ｌを生成して、識別子送信手段１６へ送る（ステップＳ２）。送信側認証・鍵交換手段１３は、このＫｃをＶＴＲ装置２に送信するために、受信側認証・鍵交換手段２３との認証・鍵交換を行う（ステップＳ３、Ｓ４）。このとき、識別子送信手段１６は、送信されるＫｃに対応するＬを識別子認識手段２５へ送信する。ＶＴＲ装置２側では、受信側認証・鍵交換手段２３は、受信したＫｃを鍵復元手段２２へ送り、識別子認識手段２５は、受信したＬを識別子記憶手段２６に送り、記憶させる（ステップＳ５）。このとき、識別子記

憶手段２６は、記憶していた旧いＬに上書き記憶するものとする。

一方、ＳＴＢ１側においては、暗号化手段１１がワークキーＫｗを生成し（ステップＳ６）、これを鍵暗号化手段１２へ送る。鍵暗号化手段１２は、ＫｗにステップＳ１で生成されたコントロールキーＫｃを用いて第２の暗号化を施して暗号化ワークキーＫｃ（Ｋｗ）に変換して、鍵復元手段２２へ送信する（ステップＳ７）。ＶＴＲ装置２側では、鍵復元手段２２は、ステップＳ４において受信側認証・鍵交換手段２３が受信したＫｃを用いて、鍵暗号化手段１２から送信されてきたＫｃ（Ｋｗ）を解読して、ワークキーＫｗを復元して、暗号解読手段２１へ送る（ステップＳ８）。

また、ＳＴＢ１側においては、暗号化手段１１が、衛星から受信した電波をＡＶデータに変換して得られたディジタルデータＤに、ステップＳ６において生成したワークキーＫｗを用いて第１の暗号化を施して暗号化ディジタルデータＫｗ（Ｄ）に変換して、暗号解読手段２１へ送信する（ステップＳ９）。ＶＴＲ装置２側では、暗号解読手段２１は、ステップＳ８において復元されたＫｗを用いて、受信したＫｗ（Ｄ）を解読して、ディジタルデータＤを復元する（ステップＳ１０）。

ＶＴＲ装置２側で、何らかの原因により受信中断が生じ、受信を再開する場合は、図３のＡに進み、受信中断が起こらない場合は、ステップＳ１２へ進む（ステップＳ１１）。受信を終了しない場合は、ステップＳ１３へ進む（ステップＳ１２）。なお、受信中断が生じ、受信を再開する場合については、追って説明する。

ステップＳ９において、１ユニットのデータの送信が終了すると、次のユニットに対してワークキーＫｗの更新を行うかどうかの判断を行い（ステッ

プＳ１３）、行う場合は、ステップＳ６に進んで、以下は、上記と同様の手順の処理を行う。Ｋｗの更新を行わない場合は、コントロールキーＫｃの更新を行うかどうかの判断を行い（ステップＳ１４）、行う場合は、ステップＳ１に進んで、以下は、上記と同様の手順の処理を行う。ただし、Ｋｃの更新を行って、Ｋｗの更新を行わない場合も存在するので、この場合は、ステップＳ６は、省略される。Ｋｃの更新を行わない場合、送信を終了する以外は、ステップＳ９に進んで（ステップＳ１５）、以下は、上記と同様の手順の処理を行う。

次に、受信中断が生じ、受信を再開する場合の手順を図３を用いて説明する。図３は、本発明の第１の実施の形態におけるデータ送受信システムにおいて、受信中断が生じ、受信を再開する場合の手順を示すフロー図である。なお、図３においても、図２の場合と同様に、左側に、ＳＴＢ１で行われる処理が、右側に、ＶＴＲ装置２で行われる処理が示されている。また、図２の場合と同様に、ＳＴＢ１とＶＴＲ装置２との間のデータの送受信は、全てＤ－Ｉ／Ｆ１４および２４を介して行われるが、以下の説明においても、この説明を省略する。

図２のステップＳ１１において、受信中断が生じ、受信を再開する場合には、識別子要求手段２７は、識別子送信手段１６に対して、識別子Ｌを送信することを要求する（ステップＳ１６）。識別子送信手段１６は、この要求を受けて、Ｌを識別子認識手段２５へ送信する（ステップＳ１７）。識別子認識手段２５は、送信されてきたＬと、ステップＳ５において、識別子記憶手段２６に記憶されたＬとを比較して、送信されてきたＬが記憶されていたＬと異なる場合は、図２のステップＳ４に進み、等しい場合は、図２のステ

ップＳ８に進む（ステップＳ１８、Ｓ１９）。ステップＳ４に進むと、識別子認識手段２５の指示により、受信側認証・鍵交換手段２３は、送信側認証・鍵交換手段１３と認証・鍵交換を行うことによって、送信されてきたＬに対応するコントロールキーＫｃを入手し（ステップＳ４）、以下は図２と同様の手順の処理を行う。また、ステップＳ８に進むと、Ｋｃ入手に関する手続は行われず、鍵復元手段２２は、受信中断前に使用していた、記憶されていたＬに対応するＫｃを用いて、暗号化ワークキーＫｃ（Ｋｗ）を解読して、ワークキーＫｗを復元する（ステップＳ８）。以下は図２と同様の手順の処理を行う。

すなわち、識別子Ｌについては、暗号化等の措置を施さずに送受信を行えるため、システムに与える負荷が高い認証・鍵交換の実行を行う前に、識別子Ｌの送受信を行い、識別子Ｌにしたがって、コントロールキーＫｃが更新されたか否かを判断し、更新されていた場合にのみ、認証・鍵交換の実行を行うことによって、システムに与える負荷を低減するものである。

図４は、本発明の第１の実施の形態におけるデータ送受信システムのコントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。図の横方向は、時間の経過を表し、一段目の帯は、ＳＴＢがデータ信号を送信中であることを示す。２段目の矢印は、同じコントロールキーＫｃが使用されている範囲を示し、本図では途中でＫｃ［１］からＫｃ［２］に更新されたことを示している。３～５段目の帯は、各ケースにおけるＶＴＲ装置が受信状態であることを示し、帯が途切れている範囲は、受信が中断状態であることを示す。また、３～５段目の縦向きの両矢印は、認証・鍵交換が実行されたことを、上向き矢印は、識別子要求手段２７が、識別子送信手段１６に対し

て、識別子Ｌを送信することを要求したことを、下向き矢印は、識別子送信手段１６が識別子Ｌを送信したことをそれぞれ示す。

ケース１のＶＴＲ装置は、受信開始後に受信中断がないため、従来例と同様に、受信開始時に認証・鍵交換を実行し、以後は、コントロールキーＫｃの更新時のみに認証・鍵交換を実行するだけでよい。ケース２のＶＴＲ装置については、従来例と同様に、受信開始後に受信中断が起こり、コントロールキーＫｃの更新後に受信を再開したため、このことを識別子Ｌの送信により確認し、従来例と同様に、改めて認証・鍵交換を実行しなければならない。ケース３のＶＴＲ装置においては、中断時間が短かったため、受信再開時にＫｃが更新されていないので、このことを識別子Ｌの送信により確認し、改めて認証・鍵交換を実行することなく、受信中断前のコントロールキーＫｃを用いて鍵復元作業を継続することができるものである。すなわち、本実施の形態におけるデータ送受信システムは、ケース３の場合に、従来例に比べて、システムに与える負荷が高い認証・鍵交換の実行回数を減らすことができるものである。

（第２の実施の形態）

以下に、本発明の第２の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、本発明のデータ受信装置が本発明の識別子要求手段を備えていないことに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

図５は、本発明の第２の実施の形態におけるデータ送受信システムの構成

を示す構成図である。本実施の形態におけるデータ送受信システムの構成が、図１の第１の実施の形態におけるデータ送受信システムの構成と異なるのは、ＶＴＲ装置２が、識別子要求手段２７を備えていないこと、ＳＴＢ１の暗号化手段１１がコントロールキーＫｃの更新が行われた後、更新されたコントロールキーＫｃに対しての認証・鍵交換が完了するまでの間は、ワークキーＫｗの更新を行わないこと、および、ＳＴＢ１の識別子送信手段１６が、定期的または不定期的に、識別子ＬをＶＴＲ装置２へ送信する機能を有することである。

なお、本実施の形態においては、識別子送信手段１６が識別子ＬをＶＴＲ装置２へ送信するタイミングは、ワークキーＫｗが更新生成される度であり、更新生成されたワークキーＫｗに対応する暗号化ワークキーＫｃ（Ｋｗ）と同時に、そのときのコントロールキーＫｃに対応する識別子Ｌを送信するものとする。しかし、これに限るものではなく、送信のタイミングは、定期的または不定期的で、Ｋｃの更新をもれなくＶＴＲ装置２へ送信できる程度に頻繁であればよい。

次に、本システムにおいて、ＳＴＢ１がデータを暗号化して送信し、ＶＴＲ装置２が暗号化されたデータを解読して使用する方法の手順について、図６、図７を用いて説明する。

まず、通常の送受信時の手順を図６を用いて説明する。図６は、本発明の第２の実施の形態におけるデータ送受信システムにおいて、ＳＴＢ１がデータを暗号化して送信し、ＶＴＲ装置２が暗号化されたデータを解読して使用する方法の手順を示すフロー図である。通常の送受信時の手順について、第１の実施の形態において説明した図２のステップＳ１～Ｓ１５と異なる点は

、ステップＳ７において、鍵暗号化手段１２が暗号化ワークキーＫｃ（Ｋｗ）を鍵復元手段２２へ送信する際に、識別子送信手段１６が、送信されるＫｃに対応するＬを識別子認識手段２５へ送信し、ステップＳ８において、識別子認識手段２５が、受信したＬを識別子記憶手段２６に送り、記憶させることである。その他は、第１の実施の形態と同様であるため、説明を省略する。

次に、受信中断が生じ、受信を再開する場合の手順を図７を用いて説明する。図７は、本発明の第２の実施の形態におけるデータ送受信システムにおいて、受信中断が生じ、受信を再開する場合の手順を示すフロー図である。なお、図７においては、特に説明のないものについては、図３の場合と同様とする。

図６のステップＳ１１において、受信中断が生じ、受信を再開する場合には、ＶＴＲ装置２側からの積極的な処理は行わず、ＳＴＢ１からのデータの送付を待つ。前述したステップＳ７と同様に、鍵暗号化手段１２が暗号化ワークキーＫｃ（Ｋｗ）を鍵復元手段２２へ送信する際に、識別子送信手段１６が、送信されるＫｃに対応するＬを識別子認識手段２５へ送信してくるので（ステップＳ６６）、識別子認識手段２５は、送信されてきたＬと、ステップＳ５またはＳ８において、識別子記憶手段２６に記憶されたＬとを比較して、送信されてきたＬが記憶されていたＬと異なる場合は、図６のステップＳ４に進み、等しい場合は、図６のステップＳ８に進む（ステップＳ６７、Ｓ６８）。ステップＳ４に進むと、識別子認識手段２５の指示により、受信側認証・鍵交換手段２３は、送信側認証・鍵交換手段１３と認証・鍵交換を行うことによって、送信されてきたＬに対応するコントロールキーＫｃを

入手し（ステップＳ４）、以下は図６と同様の手順の処理を行う。また、ステップＳ８に進むと、Ｋｃ入手に関する手続は行われず、鍵復元手段２２は、受信中断前に使用していた、記憶されていたＬに対応するＫｃを用いて、暗号化ワークキーＫｃ（Ｋｗ）を解読して、ワークキーＫｗを復元する（ステップＳ８）。以下は図６と同様の手順の処理を行う。

すなわち、識別子Ｌについては、暗号化等の措置を施さずに送受信を行えるため、システムに与える負荷が高い認証・鍵交換の実行を行う前に、識別子Ｌの送受信を行い、識別子Ｌにしたがって、コントロールキーＫｃが更新されたか否かを判断し、更新されていた場合にのみ、認証・鍵交換の実行を行うことによって、システムに与える負荷を低減するものである。

また、本実施の形態においては、ＳＴＢ１の暗号化手段１１がコントロールキーＫｃの更新が行われた後、更新されたコントロールキーＫｃに対しての認証・鍵交換が完了するまでの間は、ワークキーＫｗの更新を行わないこととしているので、認証・鍵交換の途中で行われたＫｗの更新結果を受け取れないという不具合も防止できる。

図８は、本発明の第２の実施の形態におけるデータ送受信システムのコントロールキー更新と認証・鍵交換の実行の関係を示す模式図である。図の横方向は、時間の経過を表し、一段目の帯は、ＳＴＢがデータ信号を送信中であることを示す。２段目の矢印は、同じコントロールキーＫｃが使用されている範囲を示し、本図では途中でＫｃ［１］からＫｃ［２］に更新されたことを示している。３～５段目の帯は、各ケースにおけるＶＴＲ装置が受信状態であることを示し、帯が途切れている範囲は、受信が中断状態であることを示す。また、３～５段目の縦向きの両矢印は、認証・鍵交換が実行された

ことを、下向き矢印は、識別子送信手段１６が識別子Ｌを送信したことをそれぞれ示す。前述したように、鍵暗号化手段１２が暗号化ワークキーＫｃ（Ｋｗ）を鍵復元手段２２へ送信する際に、識別子送信手段１６が、送信されるＫｃに対応するＬを識別子認識手段２５へ送信しているので、これを示す下向き矢印がＶＴＲ装置の受信状態に関わらず、頻繁に現れている。

ケース１のＶＴＲ装置は、受信開始後に受信中断がないため、従来例と同様に、受信開始時に認証・鍵交換を実行し、以後は、コントロールキーＫｃの更新時のみに認証・鍵交換を実行するだけでよい。ケース２のＶＴＲ装置については、従来例と同様に、受信開始後に受信中断が起こり、コントロールキーＫｃの更新後に受信を再開したため、このことを識別子Ｌの送信により確認し、従来例と同様に、改めて認証・鍵交換を実行しなければならない。ケース３のＶＴＲ装置においては、中断時間が短かったため、受信再開時にＫｃが更新されていないので、このことを識別子Ｌの送信により確認し、改めて認証・鍵交換を実行することなく、受信中断前のコントロールキーＫｃを用いて鍵復元作業を継続することができるものである。すなわち、本実施の形態におけるデータ送受信システムは、ケース３の場合に、従来例に比べて、システムに与える負荷が高い認証・鍵交換の実行回数を減らすことができるものである。

なお、第２の実施の形態におけるデータ送受信システムのデータ送信装置は、請求項７の本発明の機能を有するものであるとして説明したが、本機能を有さない場合においても、認証・鍵交換の実行回数を減らすことによって、送受信効率を高めるという効果はある。また、第１の実施の形態におけるデータ送受信システムのデータ送信装置が、本機能を有するものであるとし

ても、第２の実施の形態におけるデータ送受信システムと同様の効果が得られる。

また、上述した第１および第２の実施の形態におけるデータ送受信システムおよびデータ受信装置は、本発明の識別子記憶手段を備えるとして説明したが、これに限るものではなく、要するに、本発明の識別子認識手段が、少なくとも、受信中断後に受信を再開する際に、データ送信装置から送信されてきた、コントロールキーを特定するための識別子を参照することにより、前記コントロールキーが更新されたか否かを判断できる構成でありさえすればよい。

また、本発明のデータ送受信方法、データ送受信システム、データ送信装置およびデータ受信装置は、上述した第１および第２の実施の形態においては、衛星放送のＳＴＢから当該衛星放送データを録画するＶＴＲ装置へデータの送受信を行うものであるとして説明したが、これに限るものではなく、送信側がデータを暗号化して送信し、受信側が暗号化されたデータを解読して使用するものであり、暗号化に用いた鍵を、認証・鍵交換を行うことによって送信するものであればよい。

また、上述した第１および第２の実施の形態においては、本発明のデータ送受信システムを中心に説明したが、本発明のデータ送受信方法は、上記説明中で、説明された方法である。また、本発明のプログラム記録媒体は、上述した各方法の全部または一部の各機能をコンピュータに実行させるプログラムを格納したもの、例えば、図２および図３、または、図６および図７に記載のステップの全部または一部をコンピュータに実行させるプログラムを格納したものである。

さらに、上述した第１および第２の実施の形態におけるデータ送受信システムの各構成手段・構成要素の全部または一部は、ハードウェアであってもよいし、そのハードウェアの該当する機能と同じ機能を有するソフトウェアであってもよい。

（第３の実施の形態）

次に、本発明の第３の実施の形態のＡＶコンテンツ通信システムの構成を述べる。

図９に、本発明の第３の実施の形態のＡＶコンテンツ通信システムのブロック図を示す。図９に示すように、本発明の第３の実施の形態のＡＶコンテンツ通信システムは、ＡＶコンテンツ送信装置３１と、第１のＡＶコンテンツ受信装置３２と、第２のＡＶコンテンツ受信装置３３と、ＩＥＥＥ１３９４バスから構成される。なお、図９には、アンテナ３４と、モニタ３５および３６も表示する。

さて、ＡＶコンテンツ送信装置３１は、図９に示すように、受信手段３７と、暗号化手段３８と、Ｋｃｏ生成手段３９と、暗号化手法選択手段４０と、ＡＫＥ手段４１と、暗号化手法変更通知手段４２と、Ｋｃｏ要求コマンド応答手段４３と、データ転送手段４４から構成される。

受信手段３７は、ＡＶコンテンツを、ＡＶコンテンツ送信装置３１外部のアンテナ３４を介して受信する手段である。

暗号化手段３８は、基本暗号化手法と拡張暗号化手法とを使用することができるものであって、受信手段３７からのＡＶコンテンツを入力するとともに、Ｋｃｏ生成手段３９からの暗号化鍵Ｋｃｏを入力し、暗号化手法選択手段４０によって選択された暗号化手法を使用し、暗号化鍵ＫｃｏでＡＶコン

テンツを暗号化する手段である。なお、暗号化鍵Ｋｃｏで暗号化されたＡＶコンテンツをＫｃｏ（ＡＶコンテンツ）とする。また、基本暗号化手法と拡張暗号化手法との相違は、暗号化の強度が異なるということであって、拡張暗号化手法の方が基本暗号化手法よりも暗号化の強度が強いものであるとする。さらにいうと、暗号化するさいに用いる暗号化鍵Ｋｃｏを構成するデジィタル信号の長さが異なり、例えば、基本暗号化手法は、４０ビットの暗号化鍵Ｋｃｏを用いてＡＶコンテンツを暗号化する手法であって、拡張暗号化手法は、５６ビットの暗号化鍵Ｋｃｏを用いてＡＶコンテンツを暗号化する手法であるものとする。

Ｋｃｏ生成手段３９は、暗号化手段３８が受信手段３７からのＡＶコンテンツを暗号化するさいに用いる暗号化鍵Ｋｃｏを生成する手段であって、その暗号化鍵Ｋｃｏを２０秒毎に更新するものである。

暗号化手法選択手段４０は、暗号化手段３８がＡＶコンテンツを暗号化するさいに使用する暗号化手法を選択する手段である。

ＡＫＥ手段４１は、第１のＡＶコンテンツ受信装置３２との間で認証・鍵交換を行う手段であって、第１のＡＶコンテンツ受信装置３２との間で認証が成功した場合、その第１のＡＶコンテンツ受信装置３２に対して、交換鍵Ｋｅｘ（Ｅxchange Key）を発行する手段である。また同様に、ＡＫＥ手段４１は、第２のＡＶコンテンツ受信装置３３との間で認証・鍵交換を行う手段でもある。

暗号化手法変更通知手段４２は、それまでに選択していた暗号化手法からそれとは別の暗号化手法に暗号化手法の選択を変更する場合、その変更を通知する手段である。

Ｋｃｏ要求コマンド応答手段４３は、第１のＡＶコンテンツ受信装置３２および／または第２のＡＶコンテンツ受信装置３３からの、２０秒毎に更新される最新の暗号化鍵Ｋｃｏの種を送信するように要求されたコマンドを入力し、そのコマンドにしたがって暗号化鍵Ｋｃｏの種を送信する手段である。

データ転送手段４４は、ＡＶコンテンツ送信装置３１の各構成手段と第１のＡＶコンテンツ受信装置３２および／または第２のＡＶコンテンツ受信装置３３との間でのデータ通信の仲介を行う手段である。

次に、第１のＡＶコンテンツ受信装置３２は、図９に示すように、データ転送手段４５と、ＡＫＥ手段４６と、暗号化手法通知検出手段４７と、Ｋｃｏ要求コマンド発行手段４８と、Ｋｃｏ記憶手段４９と、暗号化手法記憶手段５０と、暗号解読手段５１から構成される。

データ転送手段４５は、第１のＡＶコンテンツ受信装置３２の各構成手段とＡＶコンテンツ送信装置３１との間でのデータ通信の仲介を行う手段である。

ＡＫＥ手段４６は、ＡＶコンテンツ送信装置３１との間で認証・鍵交換を行う手段であって、ＡＶコンテンツ送信装置３１との間で認証が成功した場合、そのＡＶコンテンツ送信装置３１から交換鍵Ｋｅｘを入力する手段である。

暗号化手法通知検出手段４７は、ＡＶコンテンツ送信装置３１からのＡＶコンテンツの暗号化に使用された暗号化手法がどのような暗号化手法であるのかを検出する手段である。

Ｋｃｏ要求コマンド発行手段４８は、暗号化手法通知検出手段４７によって検出された暗号化手法にしたがって、その暗号化手法に対応する暗号化鍵

Ｋｃｏの種を送信するようにＡＶコンテンツ送信装置３１に対して要求するコマンドを発行する手段である。また、Ｋｃｏ要求コマンド発行手段４８は、その要求コマンドに対応する、ＡＶコンテンツ送信装置３１からの暗号化鍵Ｋｃｏの種を入力する手段でもある。

Ｋｃｏ記憶手段４９は、あらかじめ、ＡＶコンテンツ送信装置３１からの暗号化されたＡＶコンテンツを解読するさいに必要となる所定の関数が設定されており、ＡＫＥ手段４６からの交換鍵Ｋｅｘを入力するとともに、Ｋｃｏ要求コマンド発行手段４８からの暗号化鍵Ｋｃｏの種を入力し、交換鍵Ｋｅｘと暗号化鍵Ｋｃｏとをあらかじめ設定されている関数に代入して暗号化鍵Ｋｃｏを生成し記憶する手段である。なお、その関数については後に述べることにする。

暗号化手法記憶手段５０は、暗号化手法通知検出手段４７によって検出された暗号化手法を記憶する手段である。

暗号解読手段５１は、ＡＶコンテンツ送信装置３１からの暗号化されたＡＶコンテンツを入力するとともに、Ｋｃｏ記憶手段４９からの暗号化鍵Ｋｃｏと、暗号化手法記憶手段５０からの暗号化手法とを入力し、その暗号化手法に基づいて、暗号化されたＡＶコンテンツを暗号化鍵Ｋｃｏで解読する手段である。なお、暗号解読手段５１は、基本暗号化手法と拡張暗号化手法のいずれもを使用することができるものであるとする。

次に、第２のＡＶコンテンツ受信装置３３は、図９に示すように、データ転送手段５２と、ＡＫＥ手段５３と、Ｋｃｏ要求コマンド発行手段５４と、Ｋｃｏ記憶手段５５と、暗号解読手段５６から構成される。

データ転送手段５２は、第２のＡＶコンテンツ受信装置３３の各構成手段

とＡＶコンテンツ送信装置３１との間でのデータ通信の仲介を行う手段である。

ＡＫＥ手段５３は、ＡＶコンテンツ送信装置３１との間で認証・鍵交換を行う手段であって、ＡＶコンテンツ送信装置３１との間で認証が成功した場合、そのＡＶコンテンツ送信装置３１から交換鍵Ｋｅｘを入力する手段である。

Ｋｃｏ要求コマンド発行手段５４は、基本暗号化手法に対応する暗号化鍵Ｋｃｏの種を送信するようにＡＶコンテンツ送信装置３１に対して要求するコマンドを発行する手段である。また、Ｋｃｏ要求コマンド発行手段５４は、その要求コマンドに対応する、ＡＶコンテンツ送信装置３１からの最新の暗号化鍵Ｋｃｏの種を入力する手段でもある。

Ｋｃｏ記憶手段５５は、あらかじめ、ＡＶコンテンツ送信装置３１からの暗号化されたＡＶコンテンツを解読するさいに必要となる所定の関数が設定されており、ＡＫＥ手段５３からの交換鍵Ｋｅｘを入力するとともに、Ｋｃｏ要求コマンド発行手段５４からの暗号化鍵Ｋｃｏの種を入力し、交換鍵Ｋｅｘと暗号化鍵Ｋｃｏとをあらかじめ設定されている関数に代入して暗号化鍵Ｋｃｏを生成し記憶する手段である。

暗号解読手段５６は、ＡＶコンテンツ送信装置３１からの暗号化されたＡＶコンテンツを入力するとともに、Ｋｃｏ記憶手段５５からの暗号化鍵Ｋｃｏを入力し、基本暗号化手法に基づいて、暗号化されたＡＶコンテンツを暗号化鍵Ｋｃｏで解読する手段である。なお、暗号解読手段５６は、基本暗号化手法のみを使用することができるものであるとする。いいかえると、暗号解読手段５６は、拡張暗号化手法を使用することができないものである。

次に、ＩＥＥＥ１３９４バスは、ＡＶコンテンツ送信装置３１、第１のＡＶコンテンツ受信装置３２および第２のＡＶコンテンツ受信装置３３それぞれの間で通信されるデータの伝送路である。

また、アンテナ３４は、ＡＶコンテンツ送信装置３１外部に設置され、ＡＶコンテンツを受信する手段である。モニタ３５は、第１のＡＶコンテンツ受信装置３２からのＡＶコンテンツを表示する手段であり、同様に、モニタ３６は、第２のＡＶコンテンツ受信装置３３からのＡＶコンテンツを表示する手段である。

次に、本発明の第３の実施の形態のＡＶコンテンツ通信システムの動作を述べる。

図９のＡＶコンテンツ通信システムの動作を詳しく述べる前に、以下の説明の便宜上、次に示す状況を想定し、その状況下でのＡＶコンテンツ通信システムの動作を述べることにする。

その状況とは、先ず、ＡＶコンテンツ送信装置３１がアンテナ３４からのＡＶコンテンツを拡張暗号化手法を用いて暗号化してＩＥＥＥ１３９４バスに出力しており、そのＡＶコンテンツの出力の途中から、第１のＡＶコンテンツ受信装置３２がそのＡＶコンテンツを受信して解読し、さらにその後、拡張暗号化手法を使用することができない第２のＡＶコンテンツ受信装置３３がそのＡＶコンテンツを受信して解読しようとする状況である。

さて、はじめに、ＡＶコンテンツ送信装置３１がアンテナ３４からのＡＶコンテンツを拡張暗号化手法を用いて暗号化しＩＥＥＥ１３９４バスに出力するまでのＡＶコンテンツ送信装置３１の動作を述べる。なお、ＡＶコンテンツ送信装置３１は、上述したように、拡張暗号化手法を使用することもで

きるし、基本暗号化手法を使用することもできるが、出力するＡＶコンテンツの内容をより強く保護するという目的のために、基本暗号化手法を使用して暗号化したＡＶコンテンツを出力するように要求されることがなければ、暗号化強度のより強い拡張暗号化手法を使用してＡＶコンテンツを暗号化するものとする。

先ず、暗号化手法選択手段４０は、拡張暗号化手法を選択し、受信手段３７は、ＡＶコンテンツ送信装置３１外部のアンテナ３４を介してＡＶコンテンツを受信し、暗号化手段３８は、受信手段３７からのＡＶコンテンツを入力するとともに、Ｋｃｏ生成手段３９からの暗号化鍵Ｋｃｏ１を入力し、その後、拡張暗号化手法に基づいて、暗号化鍵Ｋｃｏ１でＡＶコンテンツを暗号化する。なお、Ｋｃｏ生成手段３９からの暗号化鍵を、拡張暗号化手法に対応する暗号化鍵であることを示すために、「Ｋｃｏ１」というように記述した。また、以下では、その拡張暗号化手法とは別の基本暗号化手法に対応する暗号化鍵を「Ｋｃｏ２」というように記述する。ところで、暗号化は、例えばＡＶコンテンツの一部のヘッダについては行われないものとする。つまり、ＡＶコンテンツが受信されたさいに、暗号化鍵Ｋｃｏ１がなくてもそのＡＶコンテンツのヘッダ情報は解読されるが、そのＡＶコンテンツの内容は暗号化鍵Ｋｃｏ１がなくては解読されないように暗号化が行われるものとする。また、暗号化手段３８が利用するＫｃｏ生成手段３９からの暗号化鍵Ｋｃｏ１は、上述したように２０秒毎に更新されるものとする。そして、Ｋｃｏ生成手段３９は、暗号化鍵Ｋｃｏ１がどのタイミングで更新するのかという情報として、ｏｄｄまたはｅｖｅｎを出力する。そのｏｄｄまたはｅｖｅｎは、互いに相手方から切り替わったときに、その切り替わりの前後でＡ

Ｖコンテンツの暗号化に使用された暗号化鍵Ｋｃｏ１が２０秒毎の更新により切り替わっていることを示すためのものであるとする。その後、データ転送手段４４は、暗号化手段３８からの暗号化鍵Ｋｃｏ１で暗号化されたＡＶコンテンツ、つまりＫｃｏ（ＡＶコンテンツ）を入力するとともに、Ｋｃｏ生成手段３９からのｏｄｄまたはｅｖｅｎを入力し、図１０（ａ）に示すように、Ｋｃｏ（ＡＶコンテンツ）のヘッダのなかにｏｄｄまたはｅｖｅｎを付加してＩＥＥＥ１３９４バスに出力する。なお、図１０（ａ）は、ＡＶコンテンツ送信装置３１から送信されるＡＶコンテンツの構成図である。図１０（ｂ）については後に説明する。

次に、上述したようにしてＡＶコンテンツ送信装置３１がＡＶコンテンツを暗号化してＩＥＥＥ１３９４バスに出力しているときに、その途中から、第１のＡＶコンテンツ受信装置３２がそのＡＶコンテンツを解読するところまでのＡＶコンテンツ送信装置３１と第１のＡＶコンテンツ受信装置３２の動作を述べる。

このとき、第１のＡＶコンテンツ受信装置３２のＡＫＥ手段４６は、ＡＶコンテンツ送信装置３１のＡＫＥ手段４１に対して、認証要求を行い、ＡＫＥ手段４６およびＡＫＥ手段４１は、互いに相手方の装置の認証を行う。その認証が成功すると、ＡＫＥ手段４１は、ＡＫＥ手段４６に交換鍵Ｋｅｘを出力する。その交換鍵Ｋｅｘは、暗号化されたＡＶコンテンツを解読するさいに必要となる鍵である。それとともに、ＡＫＥ手段４１は、第１のＡＶコンテンツ受信装置３２が拡張暗号化手法を使用することができるものであることを判断し、暗号化手法の変更を行わない。なお、ＡＫＥ手段４６およびＡＫＥ手段４１が行う認証が失敗した場合、ＡＫＥ手段４１は、ＡＫＥ手段

４６に交換鍵Ｋｅｘを出力することはない。ここでは、以下の説明の便宜上、ＡＫＥ手段４６およびＡＫＥ手段４１が行う認証は成功するものとする。

そして、第１のＡＶコンテンツ受信装置３２のＡＫＥ手段４６は、データ転送手段４５を介して、ＡＫＥ手段４１からの交換鍵Ｋｅｘを入力し、Ｋｃｏ記憶手段４９に出力する。また、暗号化手法通知検出手段４７は、ＡＶコンテンツ送信装置３１からのＡＶコンテンツが拡張暗号化手法で暗号化されたものであることを検出し、その旨の情報、つまり拡張暗号化手法を暗号化手法記憶手段５０に出力し記憶させる。さらに、Ｋｃｏ要求コマンド発行手段４８は、拡張暗号化手法に対応する最新の暗号化鍵Ｋｃｏ１の種を送信するように、ＡＶコンテンツ送信装置３１のＫｃｏ要求コマンド応答手段４３に対してコマンドを発行し、そのコマンドに対応するＫｃｏ要求コマンド応答手段４３からの最新の暗号化鍵Ｋｃｏ１の種を入力して、その種をＫｃｏ記憶手段４９に出力する。なお、上述したように、ＡＶコンテンツ送信装置３１からの暗号化鍵Ｋｃｏ１が２０秒毎に更新されるので、Ｋｃｏ要求コマンド発行手段４８は、Ｋｃｏ要求コマンド応答手段４３に対するコマンドを２０秒毎に発行するものとする。その後、Ｋｃｏ記憶手段４９は、後述する（数１）に示すように、あらかじめ設定されている関数に、ＡＫＥ手段４６からの交換鍵Ｋｅｘと、Ｋｃｏ要求コマンド発行手段４８からの暗号化鍵Ｋｃｏ１の種とを代入し、暗号化鍵Ｋｃｏ１を生成し記憶する。なお、（数１）のｓｅｅｄのところに、暗号化鍵Ｋｃｏ１の種を代入する。

【数１】

Ｋｃｏ＝ｆ（ｓｅｅｄ，Ｋｅｘ）

そして、ＡＶコンテンツ送信装置３１からのＫｃｏ（ＡＶコンテンツ）のヘ

ッダのなかのｏｄｄまたはｅｖｅｎを検出し、さらに、ｏｄｄとｅｖｅｎとの切り替わりを判断して、ＡＶコンテンツ送信装置３１からのＫｃｏ（ＡＶコンテンツ）がどの暗号化鍵Ｋｃｏ１で暗号化されたのかを特定する。なお、上述したように、ｏｄｄとｅｖｅｎとの切り替わりは、その切り替わりの前後でＡＶコンテンツの暗号化に使用された暗号化鍵Ｋｃｏ１が切り替わっていることを示す。また、ＡＶコンテンツ送信装置３１のＫｃｏ要求コマンド応答手段４３は、Ｋｃｏ要求コマンド発行手段４８からの、暗号化鍵Ｋｃｏ１の種の送信要求のコマンドを入力すると、そのコマンドにしたがって、暗号化鍵Ｋｃｏ１の種をデータ転送手段４４に出力する。そして、データ転送手段４４は、図１０（ｂ）に示すように、Ｋｃｏ（ＡＶコンテンツ）に使用した暗号化鍵Ｋｃｏ１の種を、Ｋｃｏ（ＡＶコンテンツ）とは別の非同期信号を使用してコマンドでＩＥＥＥ１３９４バスに出力する。なお、図１０（ｂ）は、ＡＶコンテンツ送信装置３１から送信されるコマンドの構成図である。

最後に、暗号解読手段５１は、ＡＶコンテンツ送信装置３１からの暗号化されたＡＶコンテンツをデータ転送手段４５を介して入力するとともに、Ｋｃｏ記憶手段４９からの暗号化鍵Ｋｃｏ１と、暗号化手法記憶手段５０からの拡張暗号化手法とを入力し、その拡張暗号化手法に基づいて、暗号化されたＡＶコンテンツを暗号化鍵Ｋｃｏ１で解読し、モニタ３５に出力する。そして、モニタ３５は、暗号解読手段５１からのＡＶコンテンツの内容を表示する。

次に、上述したようにして、ＡＶコンテンツ送信装置３１が拡張暗号化手法を使用してＡＶコンテンツを暗号化して出力し、第１のＡＶコンテンツ受

信装置３２がそのＡＶコンテンツを解読しているときに、拡張暗号化手法を使用することができない第２のＡＶコンテンツ受信装置３３がそのＡＶコンテンツを解読するさいのＡＶコンテンツ送信装置３１、第１のＡＶコンテンツ受信装置３２および第２のＡＶコンテンツ受信装置３３の動作を述べる。なお、そのさいのＡＶコンテンツ送信装置３１の動作については図１１のフローチャートをも用いて説明する。

さて、第２のＡＶコンテンツ受信装置３３のＡＫＥ手段５３は、ＡＶコンテンツ送信装置３１のＡＫＥ手段４１に対して、認証要求を行い、ＡＫＥ手段５３およびＡＫＥ手段４１は、互いに相手方の装置の認証を行う（図１１のステップ１）。そのさい、ＡＫＥ手段５３は、ＡＶコンテンツ送信装置３１が出力するＡＶコンテンツの暗号化手法を、基本暗号化手法にするように要求する。なぜなら、第２のＡＶコンテンツ受信装置３３は、拡張暗号化手法を使用することができず、基本暗号化手法しか使用することができないからである。そして、互いの認証が成功すると、ＡＫＥ手段４１は、その要求を受け入れ（図１１のステップ２）、暗号化手法選択手段４０および暗号化手法変更通知手段４２に、暗号化手法を基本暗号化手法にするように制御するための情報を出力する（図１１のステップ３）。その後、ＡＫＥ手段４１は、ＡＫＥ手段５３に交換鍵Ｋｅｘを出力し、ＡＫＥ手段４１とＡＫＥ手段５３との間の認証・鍵交換は完了する（図１１のステップ４）。なお、交換鍵Ｋｅｘは、暗号化されたＡＶコンテンツを解読するさいに必要となる鍵である。また、ＡＫＥ手段５３およびＡＫＥ手段４１が行う認証が失敗した場合、ＡＫＥ手段４１は、ＡＫＥ手段５３に交換鍵Ｋｅｘを出力することもないし、暗号化手法を基本暗号化手法にするようにとの要求を受け入れること

もない。ただしここでは、以下の説明の便宜上、ＡＫＥ手段５３およびＡＫＥ手段４１が行う認証は成功するものとする。

そして、ＡＶコンテンツ送信装置３１では、暗号化手法選択手段４０が、ＡＫＥ手段４１からの、暗号化手法を基本暗号化手法にするための情報、つまり暗号化手法を変更させるための情報にしたがって、基本暗号化手法を選択し、その旨の情報を、暗号化手段３８とＫｃｏ生成手段３９とに出力する。なお、暗号化手法選択手段４０は、ＡＫＥ手段４１とＡＫＥ手段５３との間の認証・鍵交換が完了するまでに、いいかえると、ＡＫＥ手段５３が交換鍵Ｋｅｘを入力するまでに、基本暗号化手法を選択する。その後、Ｋｃｏ生成手段３９は、その暗号化手法の基本暗号化手法への変更の情報を入力した後であって、かつ、拡張暗号化手法にしたがって生成していた暗号化鍵Ｋｃｏ１の次の更新タイミングから、基本暗号化手法にしたがった暗号化鍵Ｋｃｏ２を生成し、２０秒毎に更新してゆく。また、暗号化手法変更通知手段４２は、ＡＶコンテンツの暗号化手法を拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを、第１のＡＶコンテンツ受信装置３２の暗号化手法通知検出手段４７に出力するとともに、その暗号化手法の切り替えのタイミングの情報のコマンドを暗号化手法通知検出手段４７に出力する。

その後、ＡＶコンテンツ送信装置３１の暗号化手段３８は、受信手段３７からのＡＶコンテンツを入力するとともに、Ｋｃｏ生成手段３９からの暗号化鍵Ｋｃｏ２を入力し、基本暗号化手法に基づいて、暗号化鍵Ｋｃｏ２でＡＶコンテンツを暗号化する。さらに、Ｋｃｏ生成手段３９は、暗号化鍵Ｋｃｏ２がどのタイミングで切り替わるのかという情報としてｏｄｄまたはｅｖｅｎを出力する。そして、データ転送手段４４は、暗号化手段３８からの暗

号化鍵Ｋｃｏ２で暗号化されたＡＶコンテンツ、つまりＫｃｏ（ＡＶコンテンツ）を入力するとともに、Ｋｃｏ生成手段３９からのｏｄｄまたはｅｖｅｎを入力し、Ｋｃｏ（ＡＶコンテンツ）のヘッダのなかにｏｄｄまたはｅｖｅｎを付加してＩＥＥＥ１３９４バスに出力する。

このようにＡＶコンテンツ送信装置３１からのＡＶコンテンツの暗号化手法が基本暗号化手法に切り替わると、第２のＡＶコンテンツ受信装置３３は、そのＡＶコンテンツを解読することができるようになる。そこで次に、このときの第２のＡＶコンテンツ受信装置３３がＡＶコンテンツを解読するさいの動作を述べる。

先ず、ＡＫＥ手段５３は、ＡＶコンテンツ送信装置３１のＡＫＥ手段４１からの交換鍵Ｋｅｘを、データ転送手段５２を介して入力し、Ｋｃｏ記憶手段５５に出力する。また、Ｋｃｏ要求コマンド発行手段５４は、基本暗号化手法に対応する暗号化鍵Ｋｃｏ２の種を送信するように、ＡＶコンテンツ送信装置３１のＫｃｏ要求コマンド応答手段４３に対してコマンドを発行し、そのコマンドに対応する、Ｋｃｏ要求コマンド応答手段４３からの暗号化鍵Ｋｃｏ２の種を入力して、その種をＫｃｏ記憶手段５５に出力する。その後、Ｋｃｏ記憶手段５５は、（数１）を用いて上述したようにして、あらかじめ設定されている関数に、ＡＫＥ手段５３からの交換鍵Ｋｅｘと、Ｋｃｏ要求コマンド発行手段５４からの暗号化鍵Ｋｃｏ２の種とを代入し、暗号化鍵Ｋｃｏ２を生成し記憶する。そして、ＡＶコンテンツ送信装置３１からのＫｃｏ（ＡＶコンテンツ）のヘッダのなかのｏｄｄまたはｅｖｅｎを検出し、さらに、ｏｄｄとｅｖｅｎとの切り替わりを判断して、ＡＶコンテンツ送信装置３１からのＫｃｏ（ＡＶコンテンツ）がどの暗号化鍵Ｋｃｏ２で暗号化

されたのかを特定する。

最後に、暗号解読手段５６は、ＡＶコンテンツ送信装置３１からの暗号化されたＡＶコンテンツをデータ転送手段５２を介して入力するとともに、Ｋｃｏ記憶手段５５からの暗号化鍵Ｋｃｏ２を入力し、基本暗号化手法に基づいて、暗号化されたＡＶコンテンツを暗号化鍵Ｋｃｏ２で解読し、モニタ３６に出力する。そして、モニタ３６は、暗号解読手段５６からのＡＶコンテンツの内容を表示する。

このように、ＡＶコンテンツ送信装置３１がＡＶコンテンツの暗号化手法を基本暗号化手法に変更してＡＶコンテンツを暗号化し出力すると、第２のＡＶコンテンツ受信装置３３は、そのＡＶコンテンツを解読することができるようになるが、それまで拡張暗号化手法によって暗号化されたＡＶコンテンツを受信し解読していた第１のＡＶコンテンツ受信装置３２は、そのままでは、そのＡＶコンテンツを解読することができなくなる。そこで次に、ＡＶコンテンツ送信装置３１がＡＶコンテンツの暗号化手法を基本暗号化手法に変更した場合、第１のＡＶコンテンツ受信装置３２がそのＡＶコンテンツを解読するさいの、第１のＡＶコンテンツ受信装置３２の動作を述べる。なお、そのさいの第１のＡＶコンテンツ受信装置３２の動作については図１２のフローチャートをも用いて説明する。

さてそのとき、上述したように、第１のＡＶコンテンツ受信装置３２の暗号化手法通知検出手段４７は、ＡＶコンテンツ送信装置３１の暗号化手法変更通知手段４２からの、ＡＶコンテンツの暗号化手法が拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを入力するとともに、その暗号化手法の切り替えのタイミングの情報のコマンドも入力する（図１

２のステップ１）。そして、暗号化手法通知検出手段４７は、それら２つの情報を、Ｋｃｏ要求コマンド発行手段４８と暗号化手法記憶手段５０とに出力する。その後、Ｋｃｏ要求コマンド発行手段４８は、基本暗号化手法に対応する暗号化鍵Ｋｃｏ２の種を送信するように、ＡＶコンテンツ送信装置３１のＫｃｏ要求コマンド応答手段４３に対してコマンドを発行し（図１２のステップ２）、そのコマンドに対応する、Ｋｃｏ要求コマンド応答手段４３からの暗号化鍵Ｋｃｏ２の種を入力して、その種をＫｃｏ記憶手段４９に出力する。その後、Ｋｃｏ記憶手段４９は、あらかじめ設定されている関数に、ＡＫＥ手段４６からの交換鍵Ｋｅｘと、Ｋｃｏ要求コマンド発行手段４８からの暗号化鍵Ｋｃｏ２の種とを代入し、暗号化鍵Ｋｃｏ２を生成し記憶する（図１２のステップ３）。

最後に、暗号解読手段５１は、ＡＶコンテンツ送信装置３１からの暗号化されたＡＶコンテンツをデータ転送手段４５を介して入力するとともに、Ｋｃｏ記憶手段４９からの暗号化鍵Ｋｃｏ２と、暗号化手法記憶手段５０からの基本暗号化手法とを入力する。そして、暗号解読手段５１は、基本暗号化手法を使用することができるので、その基本暗号化手法に基づいて、暗号化されたＡＶコンテンツを暗号化鍵Ｋｃｏ２で解読し、モニタ３５に出力する（図１２のステップ４）。そして、モニタ３５は、暗号解読手段５１からのＡＶコンテンツの内容を表示する。

このように、ＡＶコンテンツ送信装置３１がＡＶコンテンツの暗号化手法を基本暗号化手法に変更した場合であっても、第１のＡＶコンテンツ受信装置３２は、暗号化手法が基本暗号化手法に切り替わったという情報と、その切り替えのタイミングの情報とを入力することによって、基本暗号化手法に

よって暗号化されたＡＶコンテンツを解読することができるようになる。

ところで、ＡＶコンテンツ送信装置３１がＡＶコンテンツの暗号化手法を基本暗号化手法に変更してＡＶコンテンツを送信しているとき、第２のＡＶコンテンツ受信装置３３がそのＡＶコンテンツを解読することを中止することがある。以下に、そのような第２のＡＶコンテンツ受信装置３３がＡＶコンテンツを解読することを中止する場合のＡＶコンテンツ送信装置３１および第１のＡＶコンテンツ受信装置３２の動作を述べる。

さて、第２のＡＶコンテンツ受信装置３３がＡＶコンテンツを解読することを中止する場合、第２のＡＶコンテンツ受信装置３３のＫｃｏ要求コマンド発行手段５４は、暗号化鍵Ｋｃｏ２の種を送信するように、ＡＶコンテンツ送信装置３１のＫｃｏ要求コマンド応答手段４３に対してコマンドを発行しなくなる。つまり、Ｋｃｏ要求コマンド応答手段４３にとっては、Ｋｃｏ要求コマンド発行手段５４からのコマンドを受信しなくなるということである。このように、Ｋｃｏ要求コマンド応答手段４３は、Ｋｃｏ要求コマンド発行手段５４からのコマンドを受信しなくなると、第２のＡＶコンテンツ受信装置３３がＡＶコンテンツを解読することを中止したものと判断する。そして、Ｋｃｏ要求コマンド応答手段４３は、第２のＡＶコンテンツ受信装置３３がＡＶコンテンツを解読することを中止したことを、暗号化手法変更通知手段４２に通知する。

その後、暗号化手法変更通知手段４２は、Ｋｃｏ要求コマンド応答手段４３からの、第２のＡＶコンテンツ受信装置３３がＡＶコンテンツを解読することを中止したとする情報を入力し、その情報に基づいて、暗号化手法選択手段４０に対して、選択する暗号化手法を基本暗号化手法から拡張暗号化手

法に切り替えさせるとともに、第１のＡＶコンテンツ受信装置３２の暗号化手法通知検出手段４７に対して、暗号化手法が基本暗号化手法から拡張暗号化手法に切り替わるという情報を、その切り替えのタイミングの情報とともに出力する。このように、暗号化手法を拡張暗号化手法に切り替えるのは、上述したように拡張暗号化手法の方が基本暗号化手法よりも暗号化の強度が強く、不正な装置にＡＶコンテンツの内容を解読させないようにする防御をより強くするためである。なお、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるさい、あらかじめＡＫＥ手段４１に、第２のＡＶコンテンツ受信装置３３が基本暗号化手法しか使用することができないということを記憶させておき、その後、暗号化手法変更通知手段４２に、第２のＡＶコンテンツ受信装置３３がＡＶコンテンツを解読することを中止した場合、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるように判断させればよい。

そして、暗号化手法選択手段４０は、暗号化手法の選択を基本暗号化手法から拡張暗号化手法に再度切り替える。このように暗号化手法が拡張暗号化手法に切り替えられた後のＡＶコンテンツ送信装置３１の各構成手段は、上述した基本暗号化手法に切り替えられる前の拡張暗号化手法に基づいてＡＶコンテンツを暗号化し出力していたときと同じ動作を行う。

他方、第１のＡＶコンテンツ受信装置３２では、暗号化手法通知検出手段４７が、ＡＶコンテンツ送信装置３１の暗号化手法変更通知手段４２からの、暗号化手法が基本暗号化手法から拡張暗号化手法に切り替わるという情報と、その切り替えのタイミングの情報とを入力する。そして、その情報にしたがって、暗号解読するさいの各構成手段が動作を切り替える。その切り替

わりのタイミングは、暗号化手法が拡張暗号化手法から基本暗号化手法に切り替わったタイミングと同様であって、またその切り替え後の第１のＡＶコンテンツ受信装置３２の各構成手段は、上述した基本暗号化手法に切り替えられる前の拡張暗号化手法に基づいて暗号化されたＡＶコンテンツを解読するさいの動作と同じように動作する。

このように、ＡＶコンテンツ送信装置３１がＡＶコンテンツの暗号化手法を基本暗号化手法を使用して暗号化しＡＶコンテンツを送信しているとき、第２のＡＶコンテンツ受信装置３３がそのＡＶコンテンツを解読することを中止した場合、ＡＶコンテンツ送信装置３１は、暗号化強度のより強い拡張暗号化手法で暗号化したＡＶコンテンツを送信するように変更する。このように暗号化手法が基本暗号化手法から拡張暗号化手法に変更された場合であっても、第１のＡＶコンテンツ受信装置３２は、それに対応してそのＡＶコンテンツを解読することができる。

なお、上述した第３の実施の形態では、ＡＶコンテンツ送信装置３１の暗号化手法変更通知手段４２は、ＡＶコンテンツの暗号化手法が拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを第１のＡＶコンテンツ受信装置３２の暗号化手法通知検出手段４７に出力するとした。しかしながら、暗号化手法変更通知手段４２は、ＡＶコンテンツの暗号化手法が拡張暗号化手法から他の暗号化手法に変更するという旨の情報を暗号化手法通知検出手段４７に出力するとしてもよい。ただしこの場合、暗号化手法通知検出手段４７は、変更後の暗号化手法がどのような暗号化手法であるのかを通知するように、ＡＶコンテンツ送信装置３１に要求しなければならない。同様に、暗号化手法変更通知手段４２は、暗号化手法の拡張暗号化手法

から基本暗号化手法への切り替えのタイミングの情報をコマンドで暗号化手法通知検出手段４７に出力するとしたが、暗号化手法変更通知手段４２は、そのような暗号化手法の切り替えのタイミングの情報を暗号化手法通知検出手段４７に出力しないとしてもよい。ただしこの場合も、暗号化手法通知検出手段４７は、暗号化手法の切り替えのタイミングの情報を通知するように、ＡＶコンテンツ送信装置３１に要求しなければならない。また、暗号化手法変更通知手段４２が出力する暗号化手法の切り替えの情報や切り替えのタイミングの情報は、コマンドではなく、ＡＶコンテンツのなかに付加されたものであってもよい。

また、上述した第３の実施の形態では、ＡＶコンテンツ送信装置３１は、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるさい、暗号化手法のみがどのような暗号化手法に切り替わるのかという情報を出力し、その後、第１のＡＶコンテンツ受信装置３２から、その変更後の暗号化手法に対応する暗号化鍵Ｋｃｏの種を送信するように要求された場合、その要求にしたがって、暗号化鍵Ｋｃｏの種を送信するとした。しかしながら、ＡＶコンテンツ送信装置３１は、暗号化手法を切り替えるさい、切り替わった後の暗号化手法の情報とともに、その変更後の暗号化手法に対応する暗号化鍵Ｋｃｏの種を出力するとしてもよい。また、ＡＶコンテンツ送信装置３１は、暗号化鍵Ｋｃｏの種を出力するとしたが、暗号化鍵Ｋｃｏそのもの、または交換鍵Ｋｅｘで暗号化した暗号化鍵Ｋｃｏを出力してもよい。その場合、受信側では、種ではなく、暗号化鍵Ｋｃｏそのもの、または交換鍵Ｋｅｘで暗号化された暗号化鍵Ｋｃｏが使用されることになる。また、暗号化鍵Ｋｃｏの種はコマンドを利用して送信されるとしたが、暗号化鍵Ｋｃｏやその種は

、コマンドで送信されても、ＡＶコンテンツのなかに付加されて送信されてもよい。

また、上述した第３の実施の形態では、ＡＶコンテンツ送信装置３１のＫｃｏ生成手段３９は、２０秒毎に暗号化鍵Ｋｃｏを更新するとしたが、Ｋｃｏ生成手段３９が暗号化鍵Ｋｃｏを更新する間隔は、２０秒毎という間隔に限定されるものではない。暗号化鍵Ｋｃｏは、定期的に更新されてもよいし、不定期に更新されてもよい。

また、上述した第３の実施の形態では、ＡＶコンテンツ送信装置３１が第２のＡＶコンテンツ受信装置３３を記憶し、その第２のＡＶコンテンツ受信装置３３から、ＡＶコンテンツを解読するための暗号化鍵Ｋｃｏ２の種を要求するコマンドが来ているか否かを判断し、そのコマンドが来なくなった場合、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるとした。しかしながら、ＡＶコンテンツ送信装置３１が、第１のＡＶコンテンツ受信装置３２と第２のＡＶコンテンツ受信装置３３とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、ＡＶコンテンツを解読するための暗号化鍵Ｋｃｏの種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て拡張暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるとしてもよい。

また、上述した第３の実施の形態では、ＡＶコンテンツ送信装置３１が暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるさい、まず、ＡＶコンテンツ送信装置３１は、第２のＡＶコンテンツ受信装置３３との間で互いに認証を行い、その認証が成功すると、暗号化手法を拡張暗号化手法か

ら基本暗号化手法に切り替えるとした。しかしながら、図１３に示すように、ＡＶコンテンツ送信装置３１は、第２のＡＶコンテンツ受信装置３３からの認証要求を受信した後（図１３のステップ１）、互いの認証が成功するか否かにかかわらず、暗号化手法を拡張暗号化手法から基本暗号化手法へ変更し（図１３のステップ２）、その変更の後、認証が成功すると（図１３のステップ３）、暗号化手法を基本暗号化手法に決定するとしてもよい（図１３のステップ５）。なお、図１３のステップ３で認証が失敗すると、暗号化手法を基本暗号化手法から拡張暗号化手法に再変更して暗号化手法を決定するとしてもよい（図１３のステップ４）。

また、上述した第３の実施の形態では、ＡＶコンテンツ送信装置３１は、第２のＡＶコンテンツ受信装置３３との間で互いに認証を行い、その認証が成功した場合に、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるとした。しかしながら、ＡＶコンテンツ送信装置３１は、第２のＡＶコンテンツ受信装置３３からの認証要求を受信すると、認証が成功するか失敗するかにかかわらず、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えて、その切り替えた後の基本暗号化手法でＡＶコンテンツを暗号化して出力してもよい。ただしこの場合、ＡＶコンテンツ送信装置３１と第２のＡＶコンテンツ受信装置３３との間での認証が失敗すると、ＡＶコンテンツ送信装置３１は、第２のＡＶコンテンツ受信装置３３に交換鍵Ｋｅｘを出力しない。したがって、ＡＶコンテンツ送信装置３１からのＡＶコンテンツは、不正な装置に解読されないように保護される。他方、ＡＶコンテンツ送信装置３１が第２のＡＶコンテンツ受信装置３３からの認証要求を受信して、暗号化手法を基本暗号化手法に切り替えて暗号化したＡＶコンテンツを出力

する場合、上述した第３の実施の形態で説明したとおり、第１のＡＶコンテンツ受信装置３２は、ＡＶコンテンツ送信装置３１からの、暗号化手法が基本暗号化手法に切り替わるという情報を入力し、ＡＶコンテンツ送信装置３１からの基本暗号化手法で暗号化されたＡＶコンテンツを入力して、基本暗号化手法でそのＡＶコンテンツを解読することになる。一方その後、ＡＶコンテンツ送信装置３１は、第２のＡＶコンテンツ受信装置３３が不正であると判断した時点で、拡張暗号化手法に再変更する。

また、上述した第３の実施の形態のＡＶコンテンツ通信システムの各構成手段・構成要素の全部または一部は、ハードウェアであってもよいし、そのハードウェアの該当する機能と同じ機能を有するソフトウェアであってもよい。

さらに、請求項２５の本発明は、請求項１６から２４のいずれかに記載のＡＶコンテンツ送信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。また、請求項２８の本発明は、請求項２６または２７記載のＡＶコンテンツ受信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体である。

産業上の利用可能性

以上説明したところから明らかなように、請求項１の本発明は、コントロールキー更新によりセキュリティを高め、認証・鍵交換の実行回数を減らすことによって送受信効率を高めるデータ送受信方法を提供することができる。

また、請求項６の本発明は、コントロールキー更新によりセキュリティを高め、認証・鍵交換の実行回数を減らすことによって送受信効率を高めるデータ送信装置を提供することができる。また、請求項８の本発明は、コントロールキー更新によりセキュリティを高め、認証・鍵交換の実行回数を減らすことによって送受信効率を高めるデータ受信装置を提供することができる。さらに、請求項１４の本発明は、コントロールキー更新によりセキュリティを高め、認証・鍵交換の実行回数を減らすことによって送受信効率を高めるデータ送受信システムを提供することができる。また、請求項１５の本発明は、本発明の各装置に備えられた各構成手段の全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したプログラム記録媒体を提供することができる。

また、本発明は、ＡＶコンテンツ送信装置が第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置がそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信方法を提供することができる。

また、本発明は、第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置がそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信装置を提供することができる。

また、本発明は、上述したＡＶコンテンツ送信方法を用いたさい、第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、第１の暗号化手法を使用することができないＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、その別のＡＶコンテンツ受信装置が引き続き

そのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信方法およびＡＶコンテンツ受信方法を提供することができる。

さらに、本発明は、上述したＡＶコンテンツ送信装置が第１の暗号化手法を使用することができないＡＶコンテンツ受信装置にそのＡＶコンテンツを解読させる場合、そのＡＶコンテンツ受信装置とは別に、第１の暗号化手法で暗号化されていたＡＶコンテンツを引き続き解読するＡＶコンテンツ受信装置を提供することができる。

請　求　の　範　囲

1．　送信側が、ディジタルデータにワークキーを用いて第１の暗号化を施した暗号化ディジタルデータと、前記ワークキーにコントロールキーを用いて第２の暗号化を施した暗号化ワークキーとを送信し、受信側が、前記送信側と認証・鍵交換を行うことによって得た前記コントロールキーを用いて、受信した前記暗号化ワークキーを解読し、解読して得られた前記ワークキーを用いて受信した前記暗号化ディジタルデータを解読して、前記ディジタルデータを得るデータ送受信方法において、前記送信側は、前記コントロールキーを定期的または不定期的に更新するとともに、前記コントロールキー毎に前記コントロールキーを特定できる識別子を付与し、前記受信側は、受信中断後に受信を再開する際に、前記送信側から送信されてきた前記識別子を参照することにより、前記受信中断中に前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記認証・鍵交換を改めて行うことによって、更新後の前記コントロールキーを得ることを特徴とするデータ送受信方法。

2．　前記受信側は、前記送信側に対して、受信中断後に受信を再開する際に、前記識別子の送信を要求し、前記送信側は、前記認証・鍵交換を行う際に前記識別子を送信するのに加えて、前記要求に応じても前記識別子を送信することを特徴とする請求項１記載のデータ送受信方法。

3．　前記送信側は、定期的または不定期的に、前記識別子を前記受信側へ送信することを特徴とする請求項１記載のデータ送受信方法。

4．　前記送信側は、前記ワークキーを定期的または不定期的に更新し、前記ワークキーに前記第１の暗号化を施す際に用いた前記コントロールキー

に対応する前記識別子を、前記ワークキーとともに前記受信側へ送信することを特徴とする請求項３記載のデータ送受信方法。

５．　前記送信側は、前記コントロールキーの更新を行った後、更新された前記コントロールキーに対しての前記認証・鍵交換が完了するまでの間は、前記ワークキーの更新を行わないことを特徴とする請求項１から４のいずれかに記載のデータ送受信方法。

６．　ワークキーを定期的または不定期的に更新生成し、ディジタルデータに前記ワークキーを用いて第１の暗号化を施して暗号化ディジタルデータに変換して、データ受信装置へ送信する暗号化手段と、

コントロールキーを定期的または不定期的に更新生成し、前記ワークキーに前記コントロールキーを用いて第２の暗号化を施して暗号化ワークキーに変換して、前記データ受信装置へ送信する鍵暗号化手段と、

前記データ受信装置との認証・鍵交換を行う送信側認証・鍵交換手段と、

前記コントロールキーを特定できる識別子を生成する識別子生成手段と、

前記識別子を前記データ受信装置へ送信する識別子送信手段とを

備えたことを特徴とするデータ送信装置。

７．　前記暗号化手段は、前記鍵暗号化手段が前記コントロールキーの更新を行った後、前記更新されたコントロールキーに対しての前記認証・鍵交換が完了するまでの間は、前記ワークキーの更新を行わないことを特徴とする請求項６記載のデータ送信装置。

８．　データ送信装置との認証・鍵交換を行う受信側認証・鍵交換手段と、

ワークキーにコントロールキーを用いて第２の暗号化を施して変換された

暗号化ワークキーを、前記受信側認証・鍵交換手段を介して得られた前記コントロールキーを用いて解読して、前記ワークキーを復元する鍵復元手段と、

ディジタルデータに前記ワークキーを用いて第１の暗号化を施して変換された暗号化ディジタルデータを、前記鍵復元手段によって復元された前記ワークキーを用いて解読して、前記ディジタルデータを復元する暗号解読手段と、

少なくとも、受信中断後に受信を再開する際に、前記データ送信装置から送信されてきた、前記コントロールキーを特定するための識別子を参照することにより、前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記受信側認証・鍵交換手段に前記認証・鍵交換を改めて行って更新後の前記コントロールキーを得ることを指示する識別子認識手段とを

備えたことを特徴とするデータ受信装置。

９．　前記識別子を記憶する識別子記憶手段を備え、前記識別子認識手段は、前記データ送信装置から送信されてきた最新の前記識別子を、前記識別子記憶手段に記憶されている、その直前に送信されてきた前記識別子と比較することによって、前記コントロールキーが更新されたか否かを判断することを特徴とする請求項８記載のデータ受信装置。

１０．　前記識別子送信手段は、前記認証・鍵交換が行われる際に前記識別子を送信するのに加えて、前記データ受信装置からの要求に応じても、前記識別子を送信することを特徴とする請求項６または７記載のデータ送信装置。

１１．　前記受信中断後に受信を再開する際に、前記識別子を送信することを前記データ送信装置に対して要求する識別子要求手段を備えることを特徴とする請求項８または９記載のデータ受信装置。

１２．　前記識別子送信手段は、定期的または不定期的に、前記識別子を前記データ受信装置へ送信することを特徴とする請求項６または７記載のデータ送信装置。

１３．　前記識別子送信手段は、前記ワークキーが更新生成される度に、前記更新生成されたワークキーに前記第２の暗号化を施す際に用いた前記コントロールキーに対応する前記識別子を、前記データ受信装置へ送信することを特徴とする請求項１２記載のデータ送信装置。

１４．　請求項６、７、１２、１３のいずれかに記載のデータ送信装置および請求項８または９記載のデータ受信装置、または、請求項１０記載のデータ送信装置および請求項１１記載のデータ受信装置を備えたことを特徴とするデータ送受信システム。

１５．　請求項６から１３のいずれかに記載のデータ送信装置またはデータ受信装置の各構成手段の全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体。

１６．　ＡＶコンテンツ送信装置が伝送路を利用して第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、

その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、

その認証要求をしたＡＶコンテンツ受信装置が使用することができる第２の暗号化手法で前記ＡＶコンテンツを暗号化して送信する

ことを特徴とするＡＶコンテンツ送信方法。

１７．　前記認証要求があったさい、既にそれまでの前記第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、前記認証要求をしたＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、

その別のＡＶコンテンツ受信装置に、暗号化手法が前記第２の暗号化手法に切り替わることを通知する

ことを特徴とする請求項１６記載のＡＶコンテンツ送信方法。

１８．　前記暗号化手法の切り替えを、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とする請求項１７記載のＡＶコンテンツ送信方法。

１９．　前記切り替えた後の前記第２の暗号化手法がどのような暗号化手法であるのかという情報を、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とする請求項１８記載のＡＶコンテンツ送信方法。

２０．　前記切り替えた後の前記第２の暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とする請求項１８記載のＡＶコンテンツ送信方法。

２１．　前記暗号化手法の切り替えのタイミングを、前記認証要求がある前に使用していた前記第１の暗号化手法での暗号化鍵の更新のタイミングとすることを特徴とする請求項１６記載のＡＶコンテンツ送信方法。

２２．　少なくとも前記別のＡＶコンテンツ受信装置に、前記暗号化手法が前記第２の暗号化手法に切り替わることを通知するとともに、その暗号化

手法の切り替えのタイミングの情報を送信することを特徴とする請求項１７記載のＡＶコンテンツ送信方法。

２３．　前記ＡＶコンテンツ送信装置が前記認証要求をしたＡＶコンテンツ受信装置を記憶し、

そのＡＶコンテンツ受信装置から、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなった場合、

前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替える

ことを特徴とする請求項１６記載のＡＶコンテンツ送信方法。

２４．　前記ＡＶコンテンツ送信装置が、前記認証要求をしたＡＶコンテンツ受信装置と前記そのＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、

前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第１の暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、

前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替える

ことを特徴とする請求項１６記載のＡＶコンテンツ送信方法。

２５．　請求項１６から２４のいずれかに記載のＡＶコンテンツ送信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体。

２６．　請求項１６から２４のいずれかに記載のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツを受信し、

そのＡＶコンテンツが暗号化されたさいに使用された暗号化手法に基づくとともに、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読する

ことを特徴とするＡＶコンテンツ受信方法。

２７．　請求項１６から２４のいずれかに記載のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、

その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、

前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記暗号化手法の切り替えに関する情報に含まれていないものを送信するように要求する

ことを特徴とする請求項２６記載のＡＶコンテンツ受信方法。

２８．　請求項２６または２７記載のＡＶコンテンツ受信方法の各ステップの全部または一部の各機能をコンピュータに実行させるためのプログラムを格納したことを特徴とするプログラム記録媒体。

２９．　送信しようとするＡＶコンテンツを暗号化するさいの暗号化手法を選択する暗号化手法選択手段と、

その暗号化手法選択手段によって選択された暗号化手法に対応した、ＡＶ

コンテンツを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、

ＡＶコンテンツを入力するとともに、前記暗号化鍵生成手段からの前記暗号化鍵を入力し、その暗号化鍵を利用して、前記ＡＶコンテンツを暗号化する暗号化手段と、

ＡＶコンテンツ受信装置との間で認証・鍵交換を行う送信側認証・鍵交換手段とを備え、

ＡＶコンテンツ送信装置が、前記暗号化手法選択手段によって選択された第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、

その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、前記送信側認証・鍵交換手段は、その認証要求をしたＡＶコンテンツ受信装置との間で認証を行い、

前記暗号化手法選択手段は、暗号化手法を、前記認証要求をしたＡＶコンテンツ受信装置が使用することができる第２の暗号化手法に切り替える

ことを特徴とするＡＶコンテンツ送信装置。

３０．　前記認証要求があったさい、既にそれまでの前記第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、前記認証要求をしたＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、

その別のＡＶコンテンツ受信装置に、暗号化手法が前記第２の暗号化手法に切り替わることを通知する暗号化手法通知手段を備えた

ことを特徴とする請求項２９記載のＡＶコンテンツ送信装置。

３１．　前記暗号化鍵生成手段は、定期的または不定期に前記暗号化鍵を更新し、

前記暗号化手法選択手段が暗号化手法を前記第２の暗号化手法に切り替え

るタイミングは、前記暗号化鍵生成手段が前記第１の暗号化手法において暗号化鍵を更新するタイミングである

ことを特徴とする請求項２９記載のＡＶコンテンツ送信装置。

３２．　前記送信側認証・鍵交換手段は、前記認証要求をしたＡＶコンテンツ受信装置を記憶するとともに、そのＡＶコンテンツ受信装置から、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなったと判断した場合、

前記暗号化手法選択手段は、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替える

ことを特徴とする請求項２９記載のＡＶコンテンツ送信装置。

３３．　前記送信側認証・鍵交換手段は、前記認証要求をしたＡＶコンテンツ受信装置と前記そのＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、

前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第１の暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、

前記暗号化手法選択手段は、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替える

ことを特徴とする請求項２９記載のＡＶコンテンツ送信装置。

３４．　請求項２９から３３のいずれかに記載のＡＶコンテンツ送信装置との間で認証・鍵交換を行う受信側認証・鍵交換手段と、

前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツのその暗号化に利用された暗号化手法の情報を入力し、記憶する暗号化手法記憶手段と、

前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツを入力するとともに、前記ＡＶコンテンツ送信装置からの暗号化鍵またはその暗号化鍵の種を入力し、その後、前記暗号化手法記憶手段に記憶されている暗号化手法に基づき、かつ、前記暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読する暗号解読手段とを備えた

ことを特徴とするＡＶコンテンツ受信装置。

３５．　請求項２９から３３のいずれかに記載のＡＶコンテンツ送信装置から送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、

その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、

前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記情報に含まれていないものを送信するように要求する要求手段を備えた

ことを特徴とする請求項３４記載のＡＶコンテンツ受信装置。

補正書の請求の範囲

［１９９９年９月２０日（２０．０９．９９）国際事務局受理：新しい請求の範囲３６，３７及び３８が加えられた。（２頁）］

３６．（追加された） 送信側は、ディジタルデータにワークキーを用いて暗号化を施した暗号化ディジタルデータを送信し、受信側は、前記送信側と認証・鍵交換を行うことによって、前記ワークキーを得るために必要なコントロールキーを得、前記コントロールキーを用いて得られた前記ワークキーを用いて、受信した前記暗号化ディジタルデータを解読し、前記ディジタルデータを得るデータ送受信方法において、

前記送信側は、前記コントロールキーを定期的または不定期的に更新するとともに、前記コントロールキー毎に前記コントロールキーを特定できる識別子を付与し、前記受信側は、受信中断後に受信を再開する際に、前記送信側から送信されてきた前記識別子を参照することにより、前記受信中断中に前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記認証・鍵交換を改めて行うことによって、更新後の前記コントロールキーを得ることを特徴とするデータ送受信方法。

３７．（追加された） ディジタルデータにワークキーを用いて暗号化を施して暗号化ディジタルデータに変換して、データ受信装置へ送信する暗号化手段と、

前記ワークキーを得るために必要なコントロールキーを定期的または不定期的に更新生成するコントロールキー更新生成手段と、

前記データ受信装置との認証・鍵交換を行う送信側認証・鍵交換手段と、

前記コントロールキーを特定できる識別子を生成する識別子生成手段と、

前記識別子を前記データ受信装置へ送信する識別子送信手段とを

備えたことを特徴とするデータ送信装置。

３８．（追加された） ディジタルデータにワークキーを用いて暗号化を施して変換された暗号化ディジタルデータを受信する受信手段と、

データ送信装置との認証・鍵交換を行う受信側認証・鍵交換手段と、

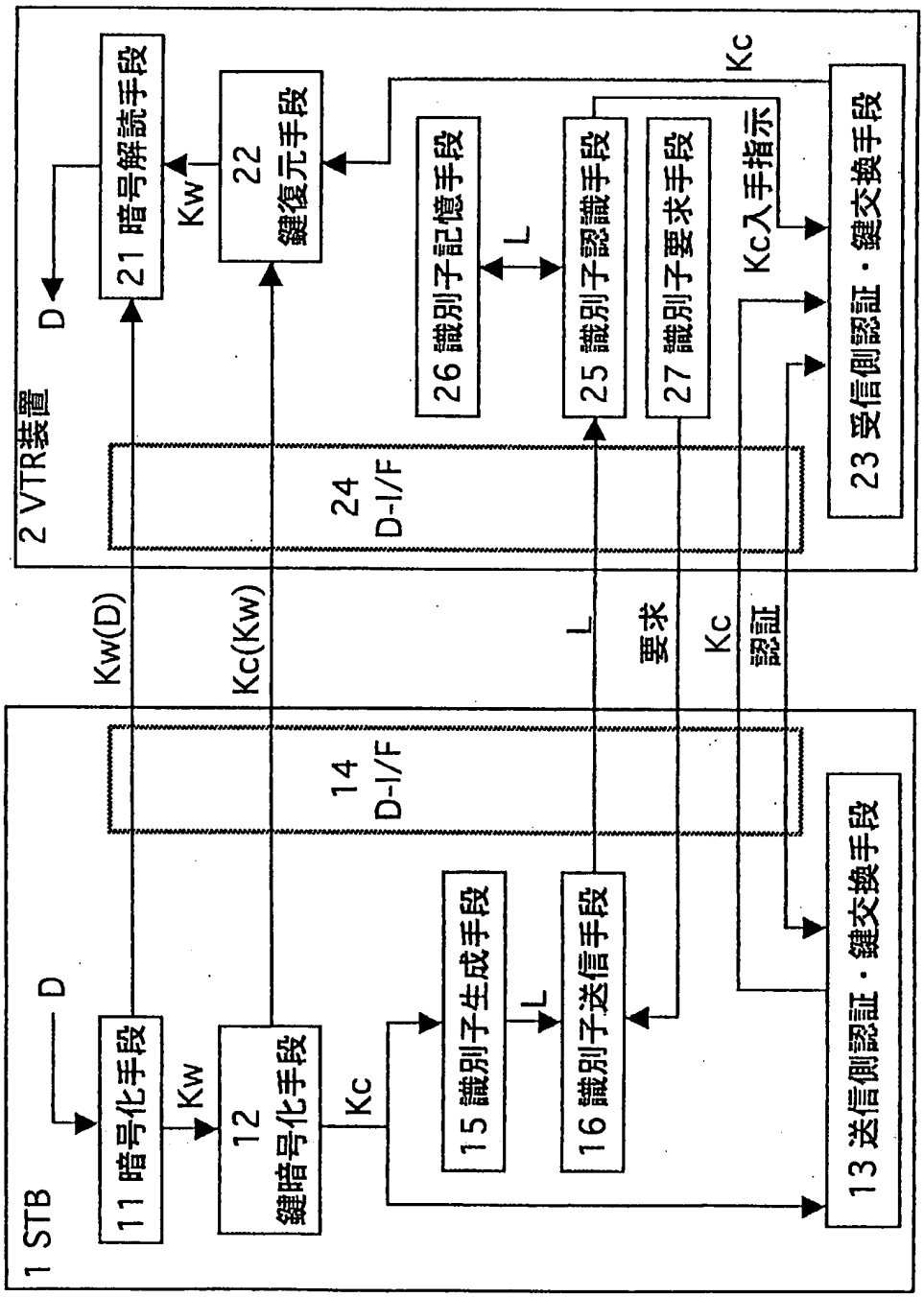
前記ワークキーを得るために必要なコントロールキーを、前記受信側認証・鍵交換手段を介して得るためコントロールキー取得手段と、

前記暗号化ディジタルデータを、前記コントロールキーを用いて生成した前記ワークキーを用いて解読して、前記ディジタルデータを復元する暗号解読手段と、

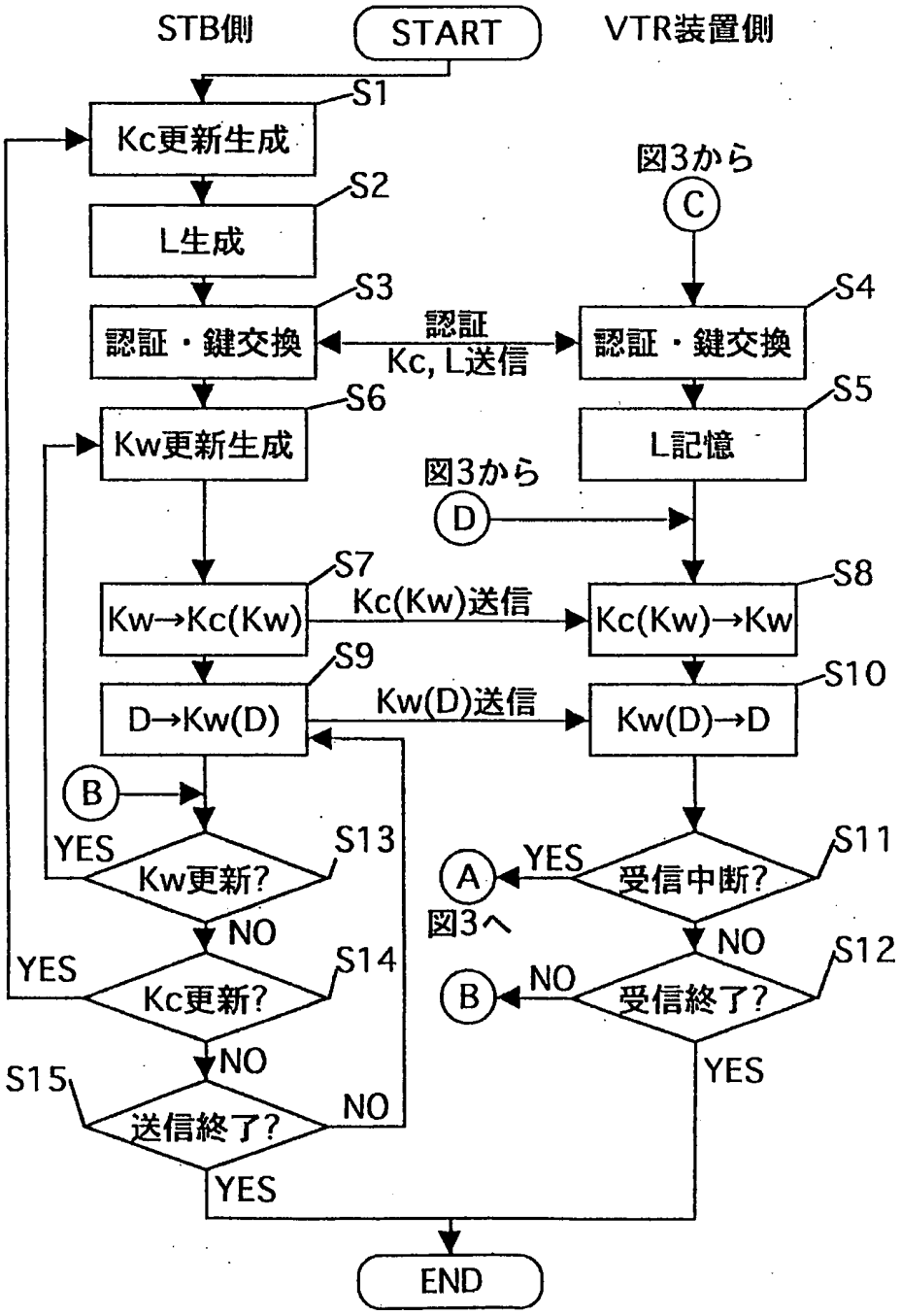
少なくとも、受信中断後に受信を再開する際に、前記データ送信装置から送信されてきた、前記コントロールキーを特定するための識別子を参照することにより、前記コントロールキーが更新されたか否かを判断し、前記コントロールキーが更新されたと判断した場合には、前記受信側認証・鍵交換手段に前記認証・鍵交換を改めて行って更新後の前記コントロールキーを得ることを指示する識別子認識手段とを

備えたことを特徴とするデータ受信装置。

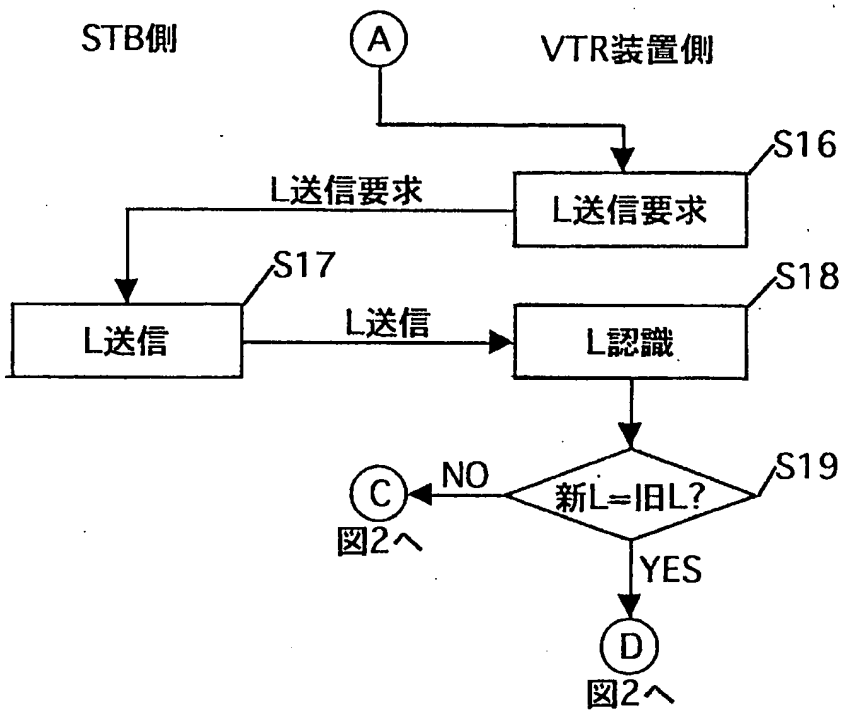
第１図


1 STB
11 暗号化手段
12 鍵暗号化手段
13 送信側認証・鍵交換手段
14 D-I/F
15 識別子生成手段
16 識別子送信手段
2 VTR装置
21 暗号解読手段
22 鍵復元手段
23 受信側認証・鍵交換手段
24 D-I/F
25 識別子認識手段
26 識別子記憶手段
27 識別子要求手段
D
Kw
Kc
L
Kw(D)
Kc(Kw)
要求
認証
Kc入手指示

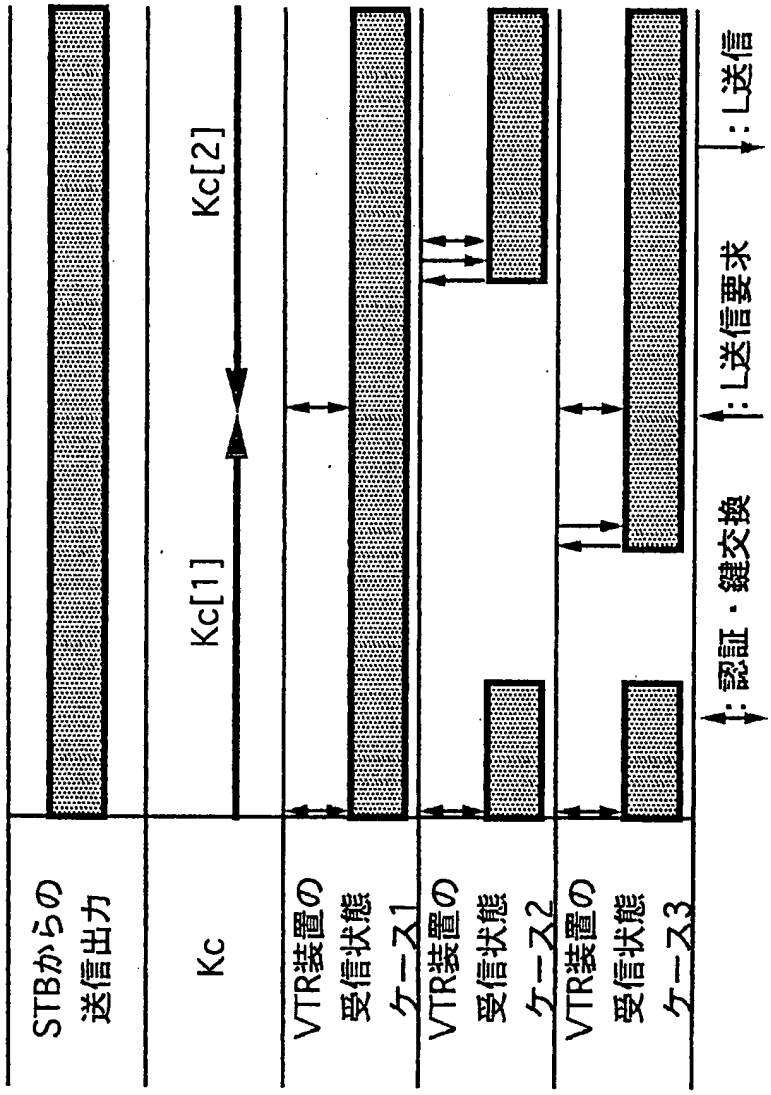
第２図


STB側
START
VTR装置側
S1
Kc更新生成
図3から
C
S2
L生成
S3
認証・鍵交換
認証
Kc, L送信
S4
認証・鍵交換
S6
Kw更新生成
S5
L記憶
図3から
D
S7
Kw→Kc(Kw)
Kc(Kw)送信
S8
Kc(Kw)→Kw
S9
D→Kw(D)
Kw(D)送信
S10
Kw(D)→D
B
YES
S13
Kw更新?
YES
A
図3へ
S11
受信中断?
NO
YES
S14
Kc更新?
NO
B
NO
S12
受信終了?
NO
S15
送信終了?
NO
YES
YES
END

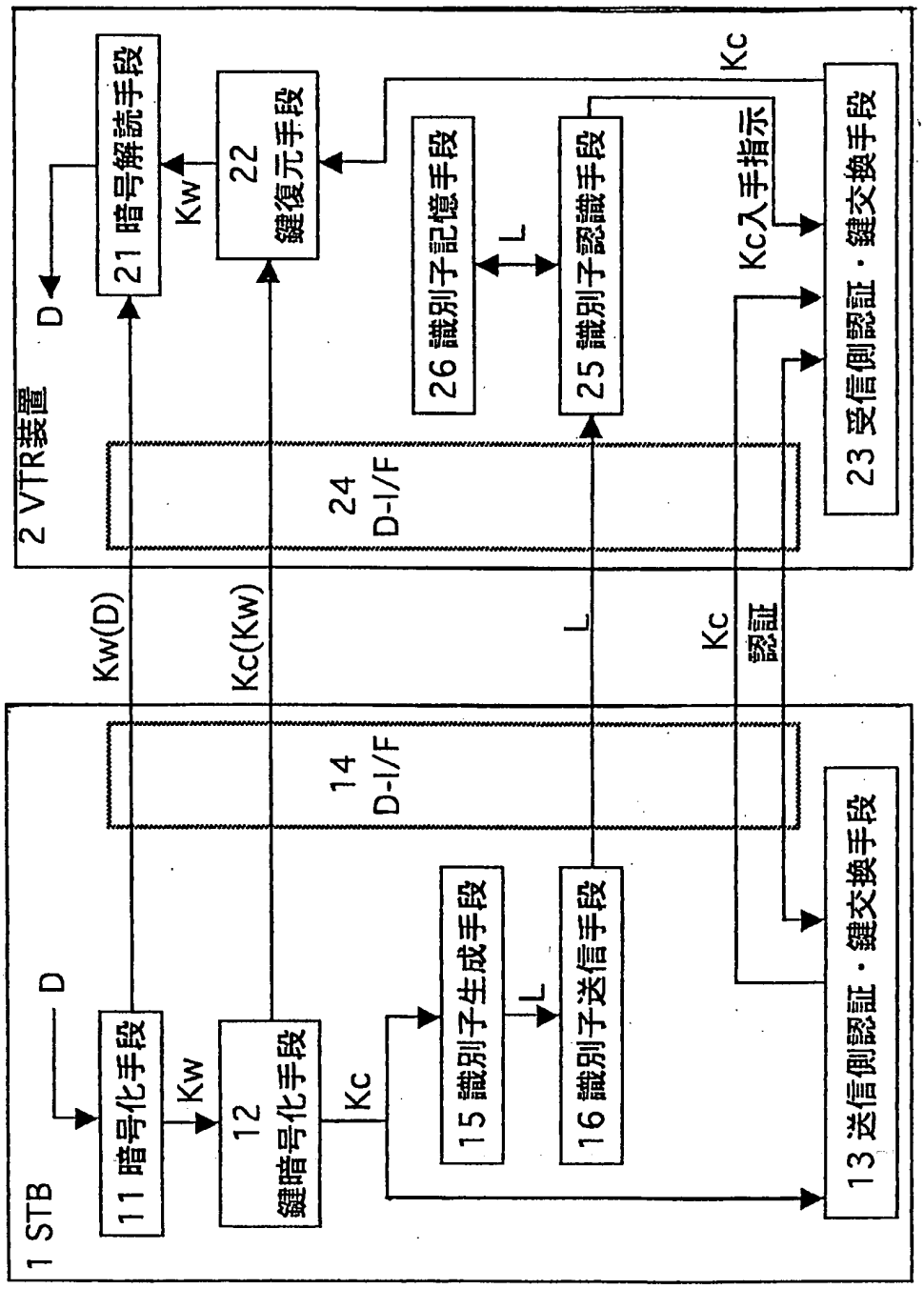
第３図


STB側
A
VTR装置側
S16
L送信要求
L送信要求
S17
S18
L送信
L送信
L認識
S19
NO
新L=旧L?
C
図2へ
YES
D
図2へ

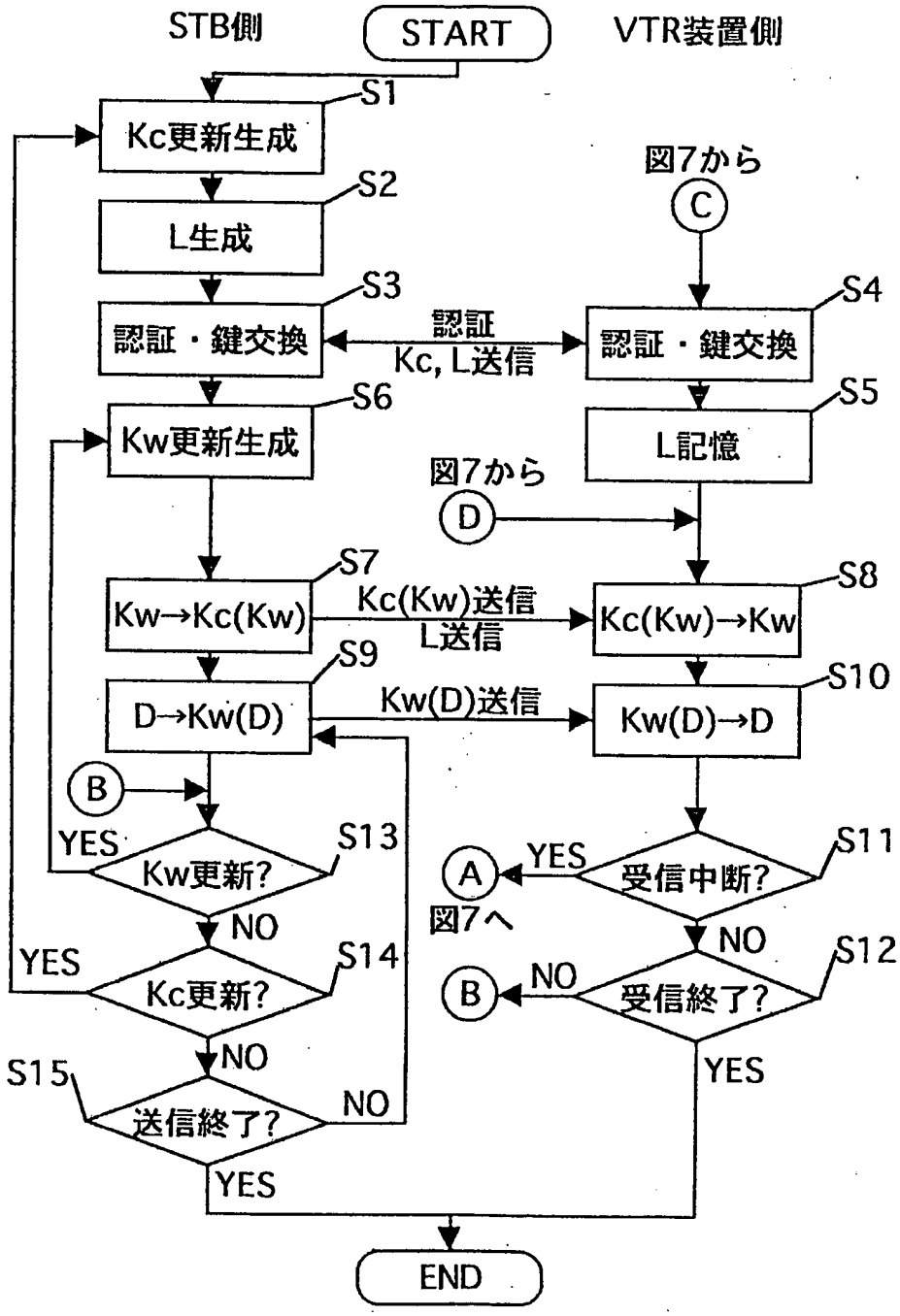
第４図


STBからの
送信出力
Kc
Kc[1]
Kc[2]
VTR装置の
受信状態
ケース1
VTR装置の
受信状態
ケース2
VTR装置の
受信状態
ケース3
：認証・鍵交換
：L送信要求
：L送信

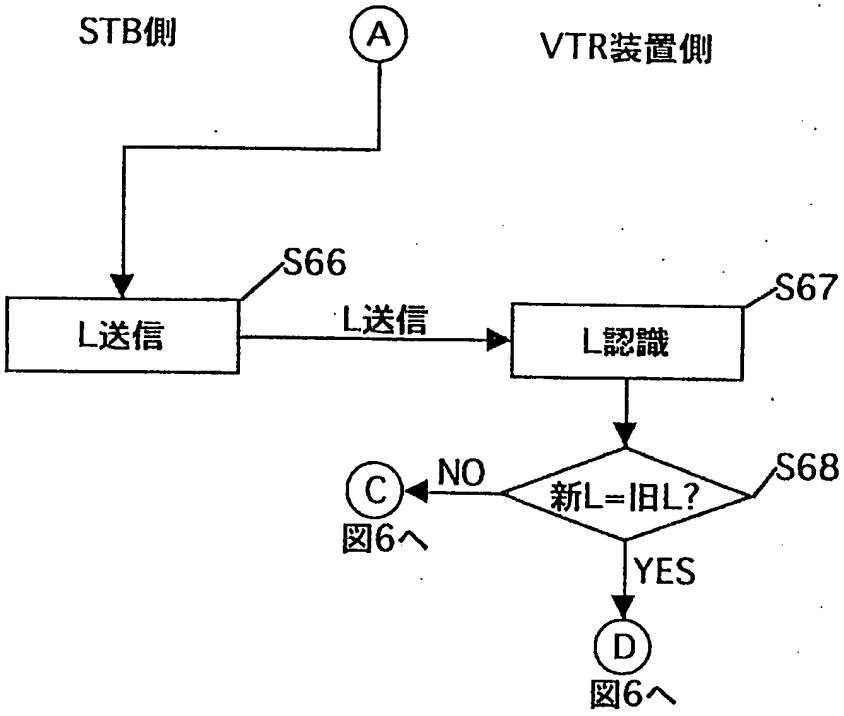
第５図


1 STB
11 暗号化手段
12 鍵暗号化手段
15 識別子生成手段
16 識別子送信手段
13 送信側認証・鍵交換手段
14 D-I/F
2 VTR装置
21 暗号解読手段
22 鍵復元手段
26 識別子記憶手段
25 識別子認識手段
24 D-I/F
23 受信側認証・鍵交換手段
D
Kw
Kc
L
Kw(D)
Kc(Kw)
Kc入手指示
認証

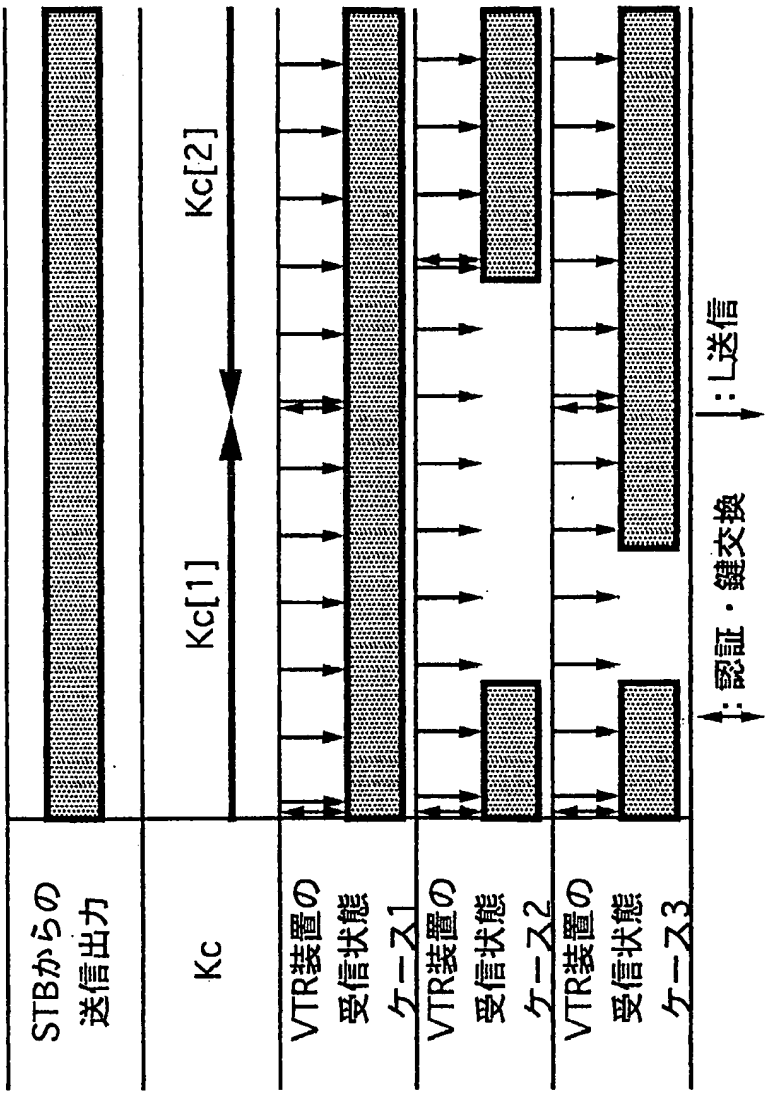
第 6 図


STB側
START
VTR装置側
S1
Kc更新生成
S2
L生成
S3
認証・鍵交換
認証
Kc, L送信
S4
認証・鍵交換
図7から
C
S5
L記憶
S6
Kw更新生成
図7から
D
S7
Kw→Kc(Kw)
Kc(Kw)送信
L送信
S8
Kc(Kw)→Kw
S9
D→Kw(D)
Kw(D)送信
S10
Kw(D)→D
B
YES
S13
Kw更新?
NO
YES
S14
Kc更新?
NO
S15
送信終了?
NO
YES
A
図7へ
YES
S11
受信中断?
NO
B
NO
S12
受信終了?
YES
END

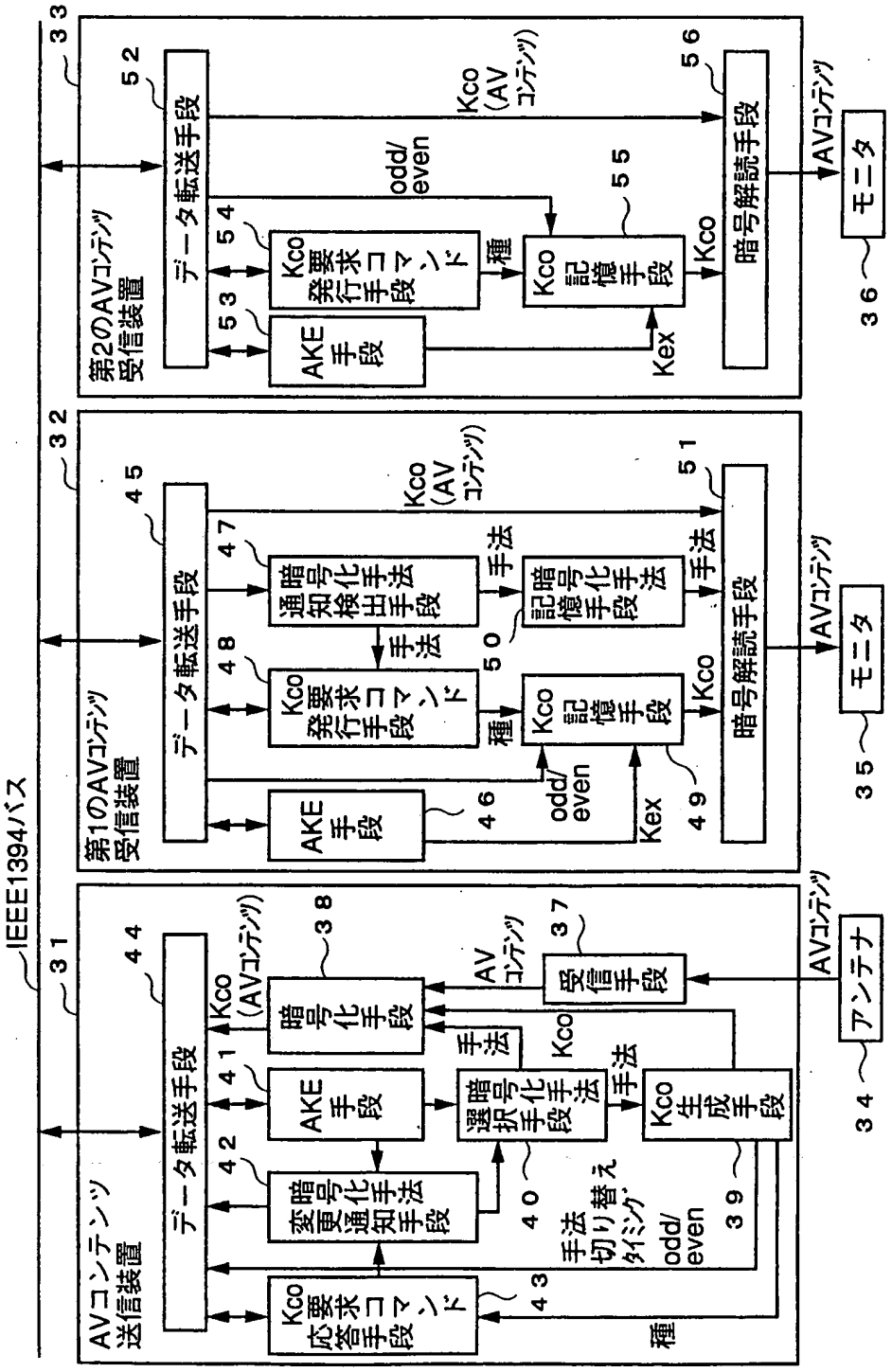
第７図



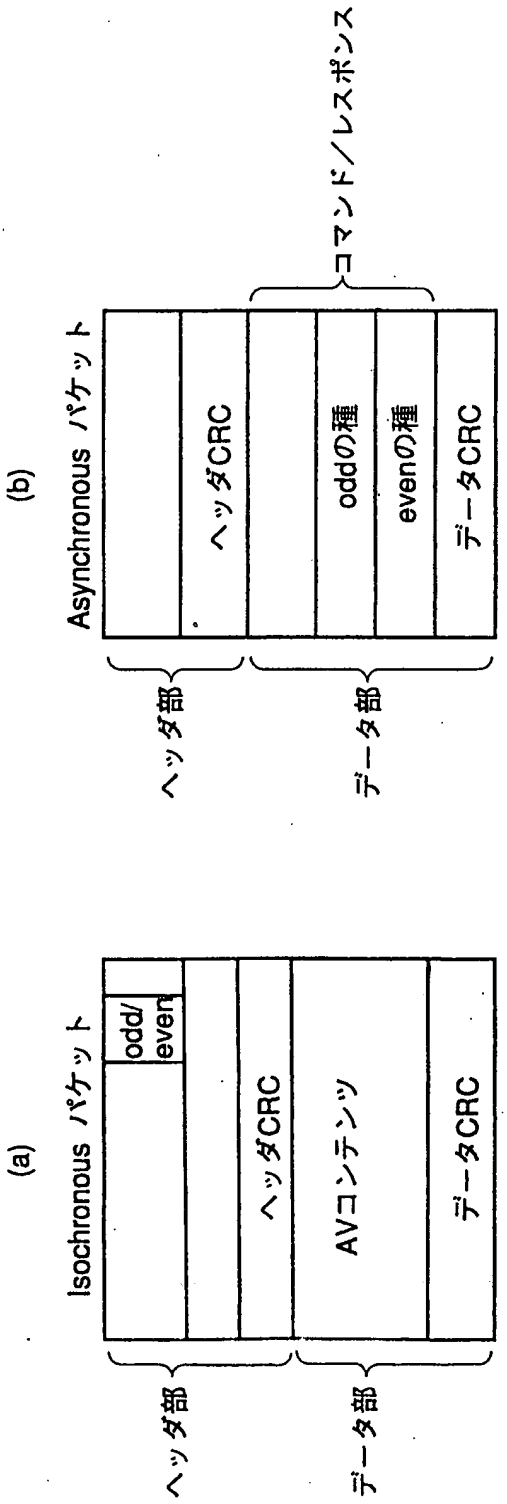
第８図


STBからの送信出力
Kc
Kc[1]
Kc[2]
VTR装置の受信状態ケース1
VTR装置の受信状態ケース2
VTR装置の受信状態ケース3
：認証・鍵交換
：L送信

第９図

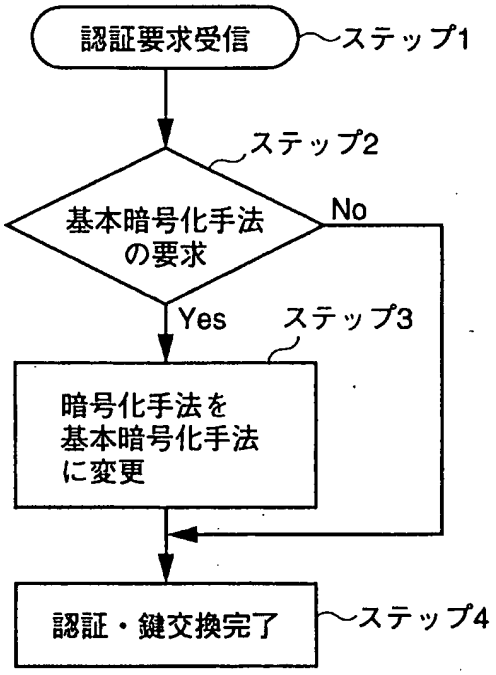

IEEE1394バス
31
AVコンテンツ送信装置
データ転送手段
44
Kco要求応答手段
43
変暗号化通知手段
42
AKE手段
41
暗号化手段
38
Kco (AVコンテンツ)
AVコンテンツ
37
受信手段
AVコンテンツ
アンテナ
34
選暗号化手段選択手法
40
Kco生成手段
39
手法
Kco
手法
種
手法切り替えタイミング
odd/even
32
第1のAVコンテンツ受信装置
データ転送手段
45
AKE手段
46
Kco発要求行手段コマンド
48
通暗知号検出手法手段
47
記暗憶号化手段手法
50
Kco記憶手段
49
暗号解読手段
51
Kco (AVコンテンツ)
AVコンテンツ
モニタ
35
odd/even
Kex
種
Kco
手法
33
第2のAVコンテンツ受信装置
データ転送手段
52
AKE手段
53
Kco発要求行手段コマンド
54
Kco記憶手段
55
暗号解読手段
56
Kco (AVコンテンツ)
AVコンテンツ
モニタ
36
odd/even
Kex
種
Kco

第１０図

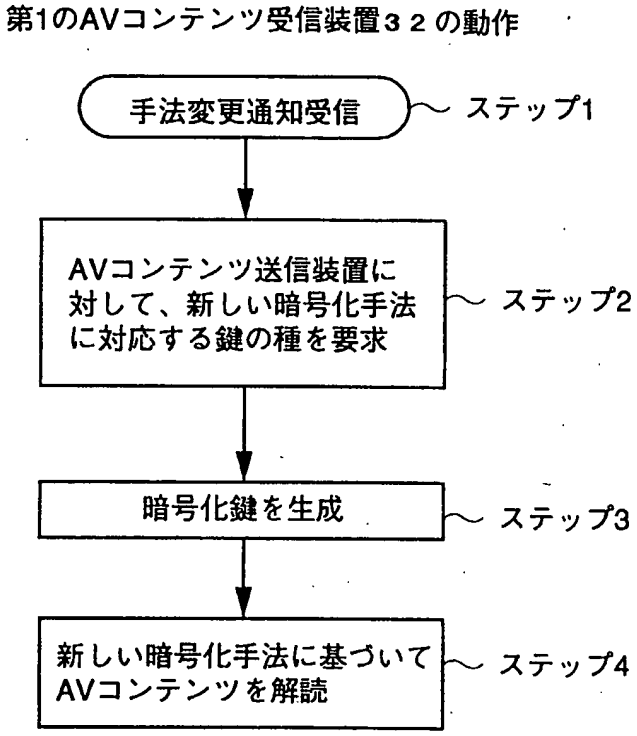

(a)
Isochronous パケット
odd/even
ヘッダCRC
AVコンテンツ
データCRC
ヘッダ部
データ部
(b)
Asynchronous パケット
コマンド／レスポンス
ヘッダCRC
oddの種
evenの種
データCRC
ヘッダ部
データ部

第１１図

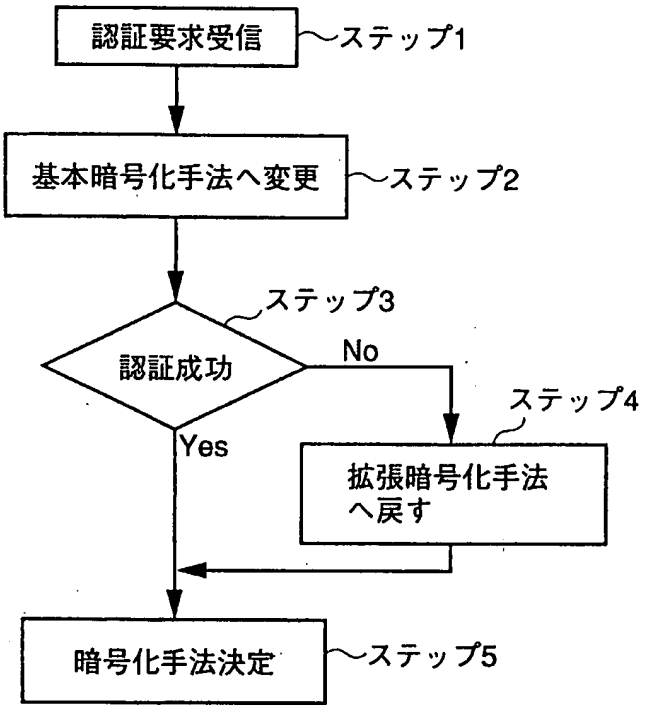
AVコンテンツ送信装置３１の動作



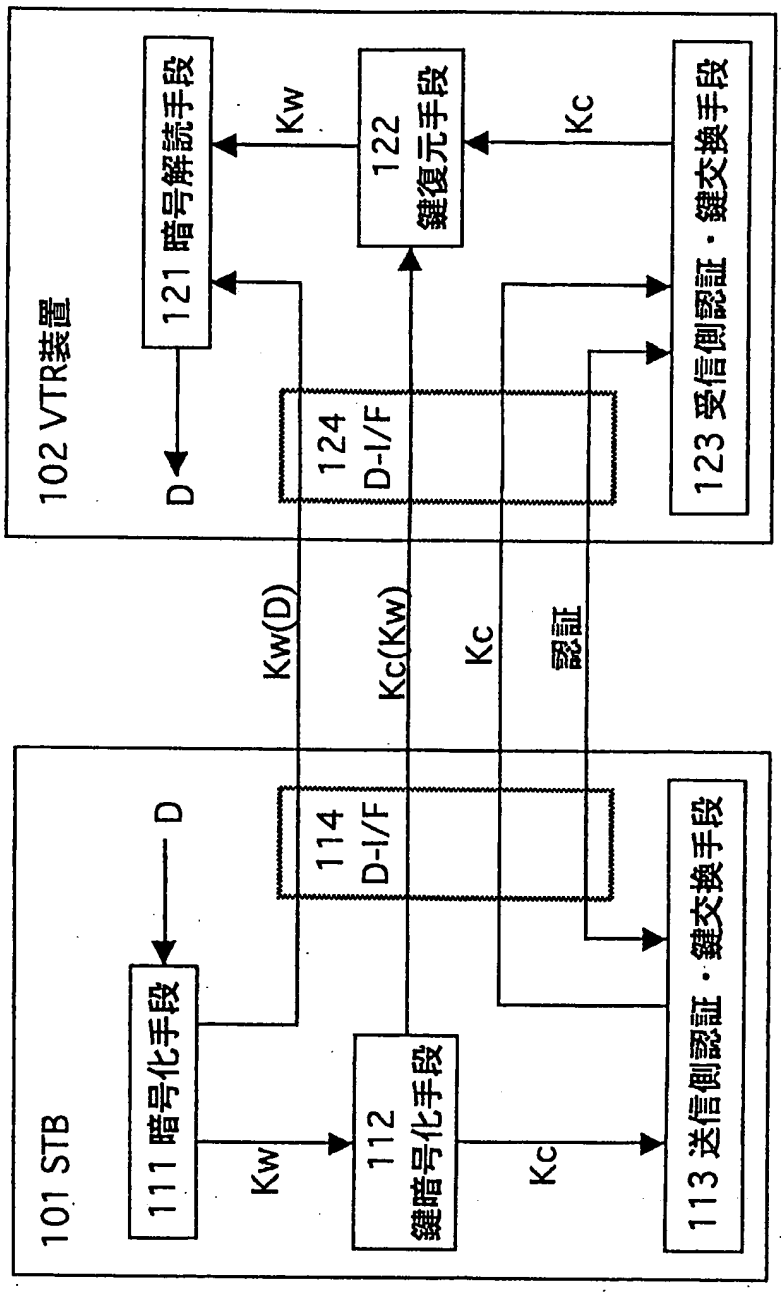
第１２図


第1のAVコンテンツ受信装置３２の動作
手法変更通知受信
ステップ1
AVコンテンツ送信装置に対して、新しい暗号化手法に対応する鍵の種を要求
ステップ2
暗号化鍵を生成
ステップ3
新しい暗号化手法に基づいてAVコンテンツを解読
ステップ4

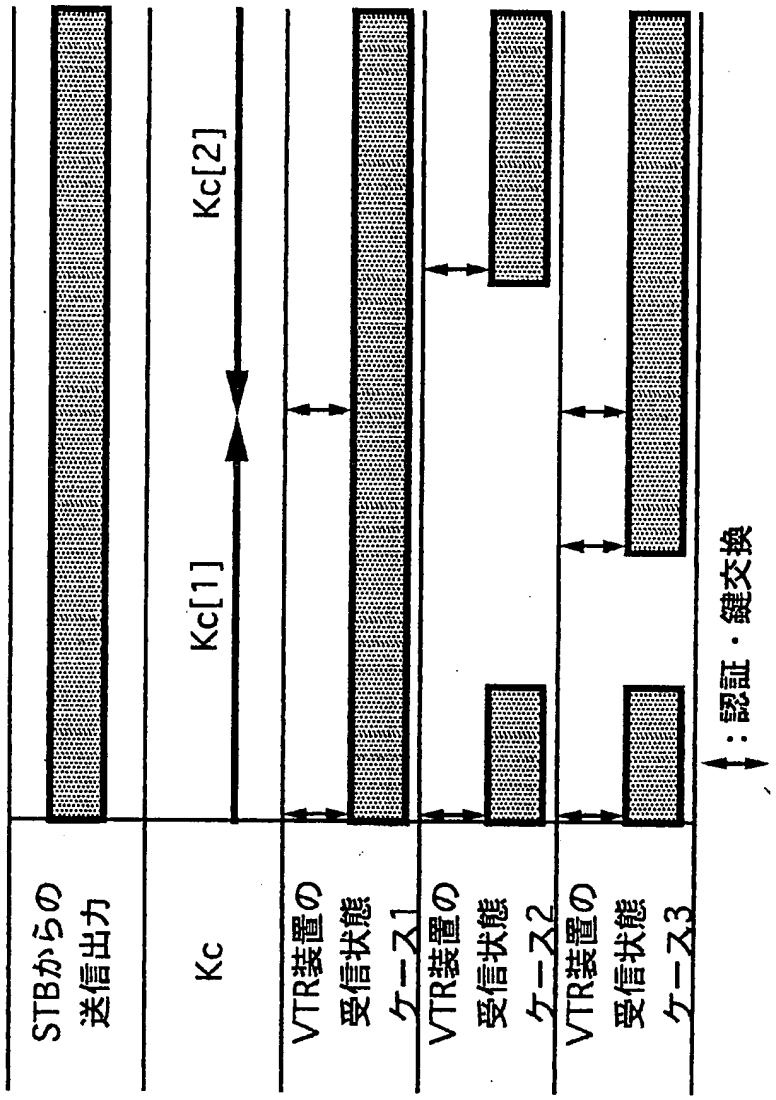
第１３図


認証要求受信
ステップ1
基本暗号化手法へ変更
ステップ2
ステップ3
認証成功
No
Yes
ステップ4
拡張暗号化手法へ戻す
暗号化手法決定
ステップ5

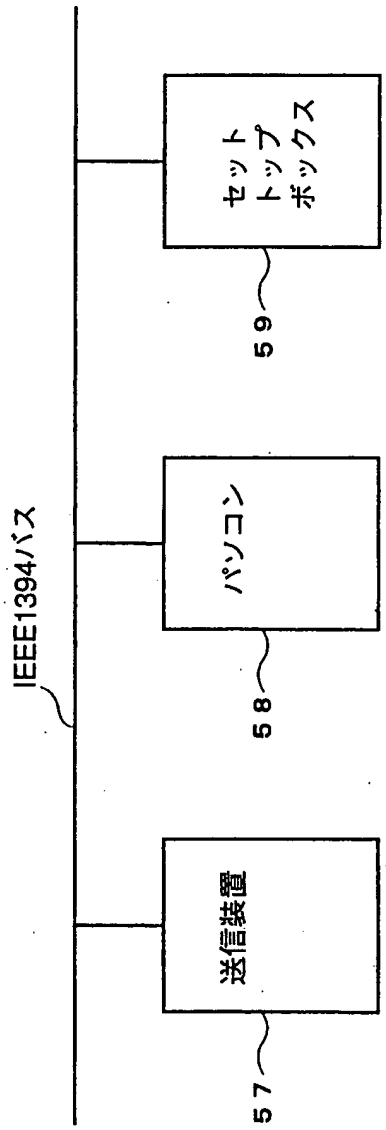
第１４図


102 VTR装置
121 暗号解読手段
122 鍵復元手段
123 受信側認証・鍵交換手段
124 D-I/F
D
Kw
Kc
Kw(D)
Kc(Kw)
Kc
認証
101 STB
111 暗号化手段
112 鍵暗号化手段
113 送信側認証・鍵交換手段
114 D-I/F
D
Kw
Kc

第１５図


STBからの送信出力
Kc
Kc[1]
Kc[2]
VTR装置の受信状態ケース1
VTR装置の受信状態ケース2
VTR装置の受信状態ケース3
：認証・鍵交換

第１６図



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/01606

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] H04L9/08, H04L9/14, H04L9/32, H04H1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] H04L9/08, H04L9/14, H04L9/32, H04H1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 63-151136, A (NEC Corp.), 23 June, 1988 (23. 06. 88), Full text ; Figs. 1 to 4 (Family: none)	1-15
Y	JP, 9-18468, A (Canon Inc.), 17 January, 1997 (17. 01. 97), Full text ; Figs. 1 to 26 & EP, 751646, A & AU, 9656198, A & JP, 9-16678, A & JP, 9-16679, A & JP, 9-18469, A & JP, 9-46329, A & CA, 2179971, A	16-35

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 July, 1999 (13. 07. 99)	21 July, 1999 (21. 07. 99)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/01606

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 9-18469, A (Canon Inc.), 17 January, 1997 (17. 01. 97), Page 3, column 3, line 48 to column 4, lines 23, 47 to page 4, column 5, lines 4, 27 to 36 ; page 5, column 7, line 40 to column 8, line 47 ; page 11, column 19, lines 5 to 23 ; Figs. 1 to 17 & EP, 751646, A & AU, 9656198, A & JP, 9-16678, A & JP, 9-16679, A & JP, 9-18468, A & JP, 9-46329, A & CA, 2179971, A	16-35
A	JP, 4-297157, A (Mitsubishi Electric Corp.), 21 October, 1992 (21. 10. 92), Full text ; Figs. 1 to 3 (Family: none)	1-15
A	JP, 59-134939, A (NEC Corp.), 2 August, 1985 (02. 08. 85), Full text ; Figs. 1 to 4 (Family: none)	16-35

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP99／01606

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁶　H04L9／08, H04L9／14, H04L9／32, H04H1／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁶　H04L9／08, H04L9／14, H04L9／32, H04H1／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－1999年
日本国登録実用新案公報	1994－1999年
日本国実用新案登録公報	1996－1999年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 63－151136, A（日本電気株式会社） 23. 6月. 1988（23. 06. 88） 全文, 第1－4図 （ファミリーなし）	1－15
Y	JP, 9－18468, A（キヤノン株式会社） 17. 1月. 1997（17. 01. 97） 全文, 図1－26 & EP, 751646, A & AU, 9656198, A & JP, 9－16678, A & JP, 9－16679, A & JP, 9－18469, A & JP, 9－46329, A & CA, 2179971, A	16－35

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 13. 07. 99	国際調査報告の発送日 21.07.99
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 青木　重徳　印　5W　4229 電話番号　03－3581－1101　内線　3576

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　PCT／JP99／01606

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP，9－18469，A（キヤノン株式会社） 17．1月．1997（17．01．97） 第3頁第3欄第48行－同頁第4欄第23行， 第3頁第4欄第47行－第4頁第5欄第4行， 第4頁第5欄第27－36行， 第5頁第7欄第40行－同頁第8欄第47行， 第11頁第19欄第5－23行，図1－17 & EP，751646，A & AU，9656198，A & JP，9－16678，A & JP，9－16679，A & JP，9－18468，A & JP，9－46329，A & CA，2179971，A	16－35
A	JP，4－297157，A（三菱電機株式会社） 21．10月．1992（21．10．92） 全文，図1－3 （ファミリーなし）	1－15
A	JP，59－134939，A（日本電気株式会社） 2．8月．1985（02．08．85） 全文，第1－4図 （ファミリーなし）	16－35

様式PCT／ISA／210（第2ページの続き）（1998年7月）